# Essential Elements of an SME-specific Search of Trusted Cloud Services

Andrea Horch[1], Constantin Christmann[2], Holger Kett[2], Jürgen Falkner[2] and Anette Weisbecker[2]
[1]*Institute of Human Factors and Technology Management IAT, University of Stuttgart, Nobelstrasse 12, Stuttgart, Germany*
[2]*Fraunhofer Institute for Industrial Engineering IAO, Nobelstrasse 12, Stuttgart, Germany*

Keywords: Cloud Computing, Cloud Services, Trust, Semantic Search, Small and Medium-sized Enterprises, SMEs.

Abstract: Cloud computing holds tremendous potential for small and medium-sized enterprises (SMEs) since it offers technologies which can improve their strategic, technical and economic situation. However, along with the benefits there are also risks which concern legal, technical and economic issues associated with cloud computing, which cause concerns to the SMEs. These concerns can be reduced by improving the transparency of cloud services including the understanding of the technology and knowledge about the service providers, already when searching for the appropriate services. To overcome these concerns and increase the transparency cloud service search systems must assist the user during the search process and provide more details about the cloud services, in particular about the attributes which influence the trust of an SME into a service and its provider. The paper introduces a solution for searching appropriate cloud services by focusing on the essential elements. A unique element in this approach is the automated monitoring and evaluation of the provided attributes of the cloud services.

## 1 INTRODUCTION

Cloud computing is an information technology model where resources, in terms of infrastructure, software applications or data are deployed via the internet by one or several service providers (Zabalza et al., 2012). Following the service model of (Mell and Grance, 2009) cloud computing products can be categorized into Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Cloud computing holds great potential for small and medium-sized enterprises (SMEs) since it can improve the strategic, technical and economic situation of an SME (Zabalza et al., 2012).

This paper focusses on the SaaS service model, which covers the provisioning of software typically in form of web applications (Mell and Grance, 2009). In order to make such cloud services accessible for customers the providers of the services have to register in a service registry or a cloud service marketplace. Whereas service repositories only provide an access and collection point for publishing and finding services, marketplaces offer a completely managed environment controlling business terms and conditions (Menychtas et al., 2011).

Along with the benefits there are also risks and legal issues associated with cloud computing causing concerns to the SMEs. The study presented by (Sahandi et al., 2012) shows the main concerns, which are a cause for the slow adoption of cloud computing by SMEs. These concerns are about security and data privacy. When outsourcing IT data, which may contain critical data like business data or customer data, security and data privacy are the key risks for an SME. The SMEs do not have control over the data which they have transferred into the cloud. As cloud services can be accessed by a web interface SMEs fear that this interface could be attacked to get unauthorized access to the application data. Another concern of the SMEs is due to the multiple data centers of the cloud service providers, which are located at different places in the world. Customers do not know at which location their data is stored and so they cannot consider the legal and regulatory issues associated with the physical location of their data.

In this paper we present the essential elements for a trusted service search for SMEs which addresses the user concerns described above. For this purpose the essential elements include in particular (1) a user query transformation and (2) an automated monitoring and evaluation of trust criteria. This paper only focuses the second point of trust monitoring and criteria.

This paper is organized as follows: Section 2


Horch A., Christmann C., Kett H., Falkner J. and Weisbecker A..
Essential Elements of an SME-specific Search of Trusted Cloud Services.
DOI: 10.5220/0004844000880094
In *Proceedings of the 4th International Conference on Cloud Computing and Services Science* (CLOSER-2014), pages 88-94
ISBN: 978-989-758-019-2

presents related work, then section 3 describes the methodology we did apply for designing a trusted service search for SMEs. In Section 4 an overview of the essential elements of the trusted search system is given and these elements are described in detail. Finally section 6 concludes with a discussion and an outlook.

## 2 RELATED WORK

An example for a cloud services search is Asperado[1], which offers a marketplace for cloud services including a service search. Asperado marketplace recommends cloud services based on user ratings and the Asperado seal of quality.

The Cloudberia website[2] acts as an open source hub for general information about cloud computing and related technologies. The website runs a service repository where everybody can register own cloud services. The repository offers an API, which acts like a proxy for the clients of the provided services.

A further registry for public cloud services is service-repository.com[3]. It contains a built-in SOAP client to browse registered services and to call their operations. For quality assurance of the registered services service-repository.com offers user ratings and a continuous availability check. Services are registered by providing the WSDL description of the service.

(Kang and Sim, 2010) present Cloudle, a multi-criteria cloud service search engine, which offers a search interface, which assists the user when searching for cloud services. The search interface proposes search criteria and search values provided by a cloud ontology.

AppDirect[4] is a cloud service marketplace and a management platform as it connects application developers with small businesses through a network of white-label marketplaces. It provides a suite of delivery solutions that enable partners to become a gateway for businesses to find, buy, and use cloud services.

Table 1 compares the related work concerning the features for improving cloud service search systems which we have proposed in section 1. The table shows that Asperado and Cloudberia do not implement requirements transformation or automated monitoring of trust criteria. Cloudle uses a cloud ontology for transforming user queries and for offering search options to assist the user during the search process. Nevertheless, the search options offered by the cloud ontology do not provide a flexible search input to the user and the user is not supported in an automated way during the specification of the functional requirements. Service-repository.com implements a monitoring of the service availability and some user ratings but other criteria relevant for the trust of users are not covered. The same holds for AppDirect as it also offers user ratings and comments leaving out other relevant trust criteria.

[1]http://marktplatz.asperado.de/

[2]http://www.cloudberia.com/

[3]http://www.service-repository.com/

[4]http://www.appdirect.com/

## 3 METHODOLOGY

Figure 1 gives an overview over the individual steps that lead to the description of essential elements for a trusted service search for SMEs as presented in this paper. As a first step we did evaluate the literature and different studies in order to get a feeling for hurdles of SMEs when adopting cloud computing. This evaluation led to the motivation (as summarized in section 1) to address the problems of cloud service adoption with a trusted service finder for SMEs. In a preliminary design step we did sketch the outline of such trusted search system. In order to get to a more detailed design we had to find solutions for the individual elements of this preliminary design. The research in this step focused two crucial features of such a search system: On the one hand, the solution for gathering user requirements in natural language and for transforming them into a formal language for service search and, on the other hand, the identification of promising approaches for an automatic monitoring of trust criteria regarding services and providers. In this paper we focus on topic 2 (Identification of approaches to monitor service criteria), topic 1 will become the key issue of further work.

## 4 ESSENTIAL ELEMENTS OF A TRUSTED SEARCH SYSTEM

The essential elements of a trusted search system we have identified are:

- Requirements collection
- User query transformation
- Trust monitoring
- Service repository
- Result presenting

Table 1: Comparison of the related work.

| | service registry | service marketplace | requirements transformation | automated monitoring of trust criteria |
|---|---|---|---|---|
| Asperado | ● | ● | ○ | ○ |
| Cloudberia | ● | ○ | ○ | ○ |
| service-repository.com | ● | ○ | ○ | ◐ |
| Cloudle | ● | ○ | ◐ | ○ |
| AppDirect | ● | ● | ○ | ◐ |

Legend: ○ not implemented, ◐ partially implemented, ● implemented

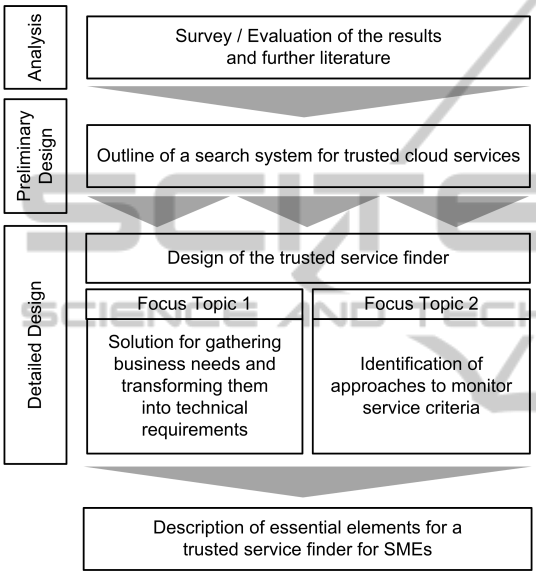


Figure 1: The applied methodology for designing a trusted search system.

In order to conduct a search the user requirements need to be gathered by the system. However, as the user may not have a high technical understanding this has to be done in a language the user is able to understand. In a second step a transformation must be applied where (based on the user input) a technical search profile is deduced, which can then be used by the system to find appropriate services. After performing the service search the result of the search must be presented to the user.

A repository is needed which stores the required attributes to describe a service. Certain attributes of a service and its provider influence the level of trust of an SME (Kett et al., 2012). It is important to increase the quality of the information of the services' attributes. Thus, techniques for trust monitoring and evaluation must be applied, which consecutively check and update service attributes automatically.

The following section describes the system element in detail, which is essential for improving trust.

# 5 TRUST MONITORING

This section describes our results regarding the identification of promising approaches for automatically monitoring trust criteria of cloud services and providers.

## 5.1 Categories of Data Sources

As a first step we tried to find adequate categories for possible data sources which can be used to gather information regarding a cloud service or its provider:

- Website of the service/provider: A website covering a cloud service or its provider offers general pieces of information. Typically only positive characteristics of a service are mentioned and eventually the information is even sugarcoated.
- Public registries (i.e. CrunchBase[5]): Such registries offer various information regarding a service or a provider in structured kind of way (i.e. year of the establishment of a company, number of employees, product overview ...). A registry is typically independent form a service/provider and the information in it is relatively trustworthy and up-to-date. Some registries also offer an Application Programming Interface (API) which makes accessing this information easy.
- Official registries (i.e. Electronical Federal Bulletin of Germany[6]): Such registries offer economic figures like the annual sales of a company. Due to the official nature of such registry this information is trustworthy - though it can be outdated. However, it depends on legal regulations if and how a service provider might be represented within such registry and which information is presented. Also automated access to the registry might not be desired.

[5]http://www.crunchbase.com/
[6]https://www.bundesanzeiger.de

- Measurements: Specific operational figures of a service can be directly measured. One example is to measure the uptime of a service by accessing a certain service URL on a regular basis.
- Review by users or experts: On the one hand the search system itself can offer an interface for user feedback regarding cloud services. On the other hand there are social networks, blogs or communities, which might offer valuable information regarding cloud services. Depending on the type of user (random user, employee of the service provider, auditor, certified accountant) the granularity varies by which such evaluation is possible and how trustworthy these results are.

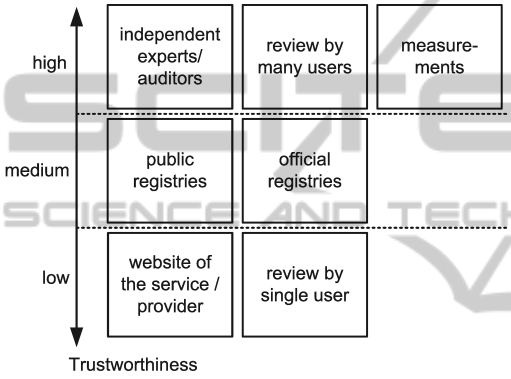


Figure 2: Weighting of the trustworthiness of different data sources for service/provider information.

In order to quantify the trustworthiness of these data sources we used a simple model where the trustworthiness of a data source is directly linked to the trustworthiness of the person/institution offering the information. Furthermore, in our model the trustworthiness is improved if a data source considers the opinions of many independent persons. Figure 2 depicts the trustworthiness of the described data sources based on this model.

## 5.2 Identification of Monitoring Approaches

For each of these data sources we have looked at the SME-specific trust factors described in (Kett et al., 2012) and tried to find automatic approaches to monitor these. The following list describes these approaches:

- Crawling of service and provider websites: The website of the cloud service and of the service provider can be crawled and relevant information can be extracted.
- Accessing public registries: Some public registries can be accessed through APIs, which offer some information regarding a service/provider.
- Monitoring of social networks and forums: Social networks and forums can be monitored by aggregating and evaluating the individual opinions regarding a service or a provider.
- Evaluation of user interface: The user interface of services can be evaluated by displaying screenshots of random services contained in the repository to users of the search services. The users can then decide if they think that the user interface is visually appealing (similar to the rating website Hot-or-Not[7]).
- Rating of trust aspects: The users of the cloud services can rate and comment the individual service descriptions. Furthermore, the assessment of such ratings and comments (as described in (Noy et al., 2005)) is now established in the internet and can also be adopted by the search system.
- Continuous benchmark: For each service a benchmark can be established (i.e. with a scripting language) which covers typical operations of this service. This benchmark can be run on a regular basis, which allows insight regarding the performance and availability. Furthermore, by checking the protocols used for communication the security of the data transfer can be monitored.
- Measuring popularity: The popularity of a service can be measured by utilizing user profiles and by keeping track of the number of users of a certain user group (i.e. the group of users working in the same business segment) signaled interested in this service. An indicator for interest could be i.e. if a user follows a link provided on the results page.
- Model-based evaluation of quality metrics: By offering the service provider the possibility to provide additional information regarding the internal processes within the service in the form of a Service Effect Specification (SEFF), this SEFF can be used by the search system to perform an evaluation of the performance (and possibly other quality metrics) using i.e. the Palladio Component Model (Rathfelder and Klatt, 2011).

## 5.3 Evaluation of Monitoring Approaches

In order to make sure that the monitored information is trustworthy on the one hand and on the other hand covers aspects of the cloud service/provider that are relevant to the users, each monitoring approach was

[7] http://www.hotornot.de/

Table 2: Evaluation of monitoring approaches regarding trustworthiness and relevance for users. The percentage value behind the trust aspects is taken from (Kasper et al., 2012) and indicates the percentage of questioned people which did assign a high relevance to this aspect. The trust level behind each data source is based on the model for the trustworthiness of the individual data sources as visualized in figure 2.

| | **Monitoring approaches** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Crawling of service and provider websites | Accessing public registries | Monitoring of social networks and forums | Evaluation of user interface | Continuous benchmark | Rating of trust aspects | Measuring popularity | Model-based evaluation of quality metrics |
| **Most relevant trust aspects based on (Kasper et al., 2012)** | | | | | | | | |
| Security of data transfer (93 %) | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ |
| Security of data storage (92 %) | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Security of data access (91 %) | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Availability / resilience (90 %) | ○ | ○ | ○ | ○ | ● | ● | ○ | ● |
| Functionality meets requirements (83 %) | ○ | ○ | ○ | ● | ○ | ● | ○ | ○ |
| Ease of use (83 %) | ○ | ○ | ○ | ● | ○ | ● | ○ | ○ |
| Clear presentation of services range (81 %) | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ |
| Performance and speed (81 %) | ○ | ○ | ○ | ○ | ● | ● | ○ | ● |
| Backup and security concept (79 %) | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Easy to start with (77 %) | ○ | ○ | ○ | ● | ○ | ● | ○ | ○ |
| **Coverage of aspects / relevance** | **10%** | **0%** | **0%** | **30%** | **30%** | **60%** | **0%** | **20%** |
| **Data sources** | | | | | | | | |
| Independent expert/auditor (h) | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Review by many users (h) | ○ | ○ | ● | ● | ○ | ● | ○ | ○ |
| Measurements (h) | ○ | ○ | ○ | ○ | ● | ○ | ● | ● |
| Public registries (m) | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ |
| Official registries (m) | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ |
| Website of the service/provider (l) | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Review by single user (l) | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| **Trustworthiness due to data source** | **l** | **m** | **h** | **h** | **h** | **h** | **h** | **h** |

Legend: ○ no assignment, ● assignment, l = low, m = medium, h = high

evaluated by determining the following two characteristics:

- Trustworthiness: The trustworthiness was derived from the trustworthiness of the involved data source (high, medium or low).
- Relevance: The relevance of the monitored information was determined based on the survey results of (Kasper et al., 2012). This study offers the percentage of questioned people which did assign a high relevance to various aspects of cloud services and providers[8]. By selecting the aspects with the highest percentage values we filtered out the 10 most relevant aspects. In order to quantify the relevance of a monitoring approach we counted how many of these 10 aspects are touched by the monitoring.

[8]The survey in (Kasper et al., 2012) was conducted by questioning employees in german craft businesses. Typically such craft businesses can be categorized as SMEs, so this survey offers insight into the weighting of trust aspects from the persective of SMEs.

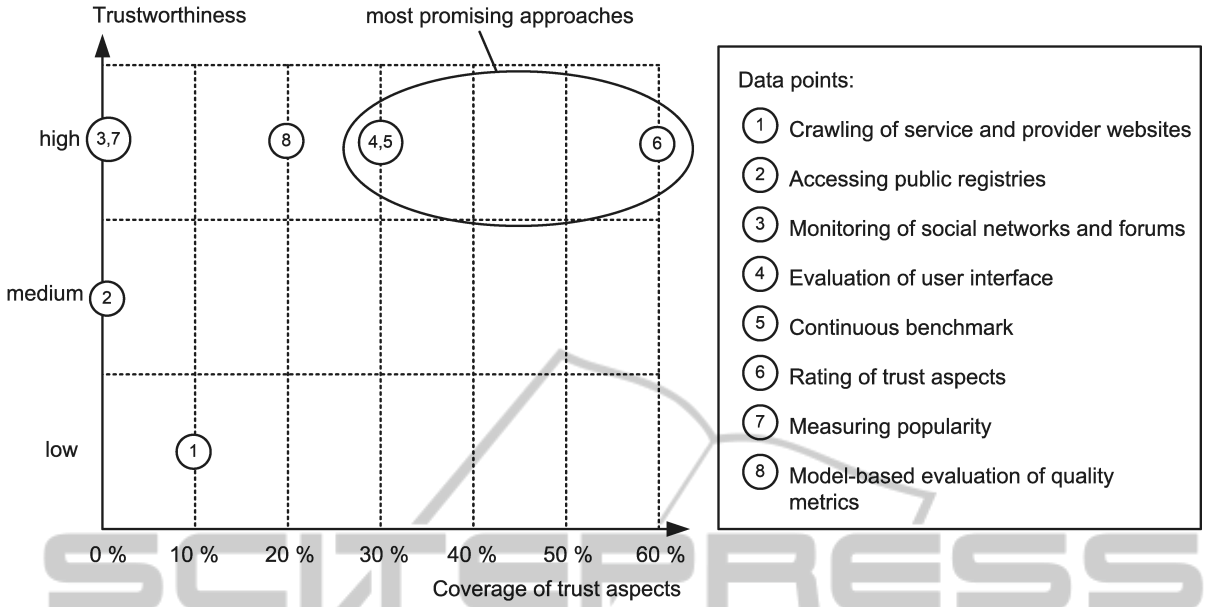


Figure 3: Distribution of monitoring approaches based on the associated trustworthiness and their coverage of trust aspects.



In table 2 the result of this evaluation is shown and figure 3 visualizes the distribution of all monitoring approaches based on this evaluation. As described in section 4 the trust monitoring is an essential element of a trusted search system and due to this distribution the rating of trust aspects by users, the evaluation of user interface and the continuous benchmark are promising approaches for this trust monitoring, as they cover relatively many important trust aspects and their data source has a high level of trust.

The most trustworthy and efficient monitoring approaches are:

1. Rating of trust aspects: For this approach the data source are the ratings of many users. There is a need for a structured approach, where every trust aspect is rated. Many user ratings produce high quality results.
2. Evaluation of user interface: This approach reflects the subjective opion of a user. It is an unstructured proceeding to get the average rating of all users regarding to functionality and usability of a service.
3. Continuous benchmark: Proceeding to get objective and reliable conclusions about trust aspects of a service.
4. Monitoring of social networks and forums: This approach holds significant potential to collect values for many trust aspects. Currently there are to less communities where data could be collected, but since there will be built up more communities in future, the data which could be collected would be a very good data source.

## 6 OUTLOOK & CONCLUSION

In this paper we have presented the essential elements for a search system for cloud services with a focus on business users from SMEs. The focus of our contribution lies on the following aspect:

- Identification of promising approaches for an automated monitoring of specific service/provider attributes which are relevant to the trust of users.

It is the intention of the authors to actually build such a search system using the described elements as guidance for its design. This development will be carried out in the context of the research project CLOUDwerker[9] and here the application domain for the implementation will be craft business. Besides the implementation of the search system we are going to examine the process of service selection of SMEs in order to better support this process by offering adequate information and guidance to potential customers of cloud services.

[9]http://www.cloudwerker.de/

## ACKNOWLEDGEMENT

This work was funded by means of the German Federal Ministry of Economy and Technology under the promotional reference “01MD11041”. The authors take the responsibility for the contents.

## REFERENCES

Kang, J. and Sim, K. M. (2010). Cloudle: A multi-criteria cloud service search engine. In *Proceedings of the 2010 IEEE Asia-Pacific Services Computing Conference*, pages 339–346. IEEE Computer Society.

Kasper, H., Kett, H., and Weisbecker, A. (2012). *Potenziale von Cloud Computing im Handwerk*. Fraunhofer-Verlag.

Kett, H., Kasper, H., Falkner, J., and Weisbecker, A. (2012). Trust factors for the usage of cloud computing in small and medium sized craft enterprises. In Vanmechelen, K., Altmann, J., and Rana, O. F., editors, *Economics of Grids, Clouds, Systems, and Services*, volume 7714 of *Lecture Notes in Computer Science*, pages 169–181. Springer-Verlag.

Mell, P. and Grance, T. (2009). The nist definition of cloud computing. Technical report, National Institute of Standards and Technology (NIST).

Menychtas, A., Gatzioura, A., and Varvarigou, T. (2011). A business resolution engine for cloud marketplaces. In *Third International Conference on Cloud Computing Technology and Science 2011 (CloudCom)*, pages 462–469. IEEE Computer Society.

Noy, N. F., Guha, R., and Musen, M. A. (2005). User ratings of ontologies: Who will rate the raters. In *Proceedings of the AAAI Spring Symposium on Knowledge Collection from Volunteer Contributors*, pages 56–63.

Rathfelder, C. and Klatt, B. (2011). Palladio workbench: A quality-prediction tool for component-based architectures. In *9th Working IEEE/IFIP Conference on Software Architecture 2011 (WICSA 2011)*, pages 347–350. IEEE Computer Society.

Sahandi, R., Alkhalil, A., and Opara-Martins, J. (2012). Smes’ perception of cloud computing: Potential and security. In Camarinha-Matos, L. M., Xu, L., and Afsarmanesh, H., editors, *Collaborative Networks in the Internet of Services*, volume 380 of *IFIP Advances in Information and Communication Technology*, pages 186–195. Springer-Verlag.

Zabalza, J., Rio-Belver, R., Cilleruelo, E., Garechana, G., and Gavilanes, J. (2012). Benefits related to cloud computing in the smes. In *6th International Conference on Industrial Engineering and Industrial Management*, pages 637–644.