Müller *et al. Journal of Cloud Computing: Advances, Systems and Applications* (2017) 6:15
DOI 10.1186/s13677-017-0082-3

Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH Open Access

Data security in decentralized cloud systems – system comparison, requirements analysis and organizational levels

André Müller[1*], André Ludwig[2] and Bogdan Franczyk[1]

Abstract

Cloud computing has been established as a technology for providing needs-orientated and use-dependent IT resources, which now are being used more frequently for business information systems. Particularly in terms of integration of decentralized information systems, cloud systems are providing a stable solution approach. Still, data security is one of the biggest challenges when using cloud systems and a main reason why many companies avoid using cloud services. The question we are facing is how cloud systems for integration of decentralized information systems have to be designed, in terms of technology and organization, so that privacy laws of the cloud user can be guaranteed. This contribution summarizes the results of a system comparison of decentralized cloud systems in social networks, a requirements analysis based on a literature analysis, and a model for organizational levels of cloud systems, derived from the requirements analysis.

Keywords: Data security, Cloud system, Decentralized information system, Requirements, Organization levels

Introduction

Cloud computing receives a lot of attention in terms of research and in practice. Over the years, the use of cloud computing in businesses has been increasing [1]. Individual infrastructure, platform and software services, which are provided by a private computer center via a private cloud system or by an external hosted private cloud system, are now being used in particular [2]. Based on cloud computing technology, new forms of IT resource relocation and their needs-orientated and use-dependent provision via commercial services have been established. Moreover, cloud computing has a far-reaching potential for the transformation of business models and operative processes, especially supported through system integration [3].

In terms of business information systems, cloud computing is becoming more and more important. Business information systems, as a socio-technological man-machine system, describe the connection between technological components and business staff, in order to fulfill the work tasks [4] and to become the backbone of many modern worlds of employment. The need for decentralization and a technological as well as an organizational new-orientation of information system is increasing because of the increasing distribution of value-added processes via various companies, a faster and more flexible new-orientation of business partnerships, and an intensive integration of customers into value-added processes [5, 6]. Current developments in information technology and communication technology, including keywords, for example, such as "Internet of Things" [7], "Cyber Physical Systems" [8], "Emergent Software Systems" [9], or "Fog Computing" [10], are supporting a higher decentralization of information systems. In this context, cloud systems are offering an infrastructural solution. Via Internet connection and the provision of software solutions and integration solutions according to the "As-a-Service-Paradigma", various decentralized components of an information system can be integrated. Though cloud systems are a stable technological basis for the

* Correspondence: amueller@wifa.uni-leipzig.de
[1] Department of Business Information Systems, Leipzig University, Grimmaische Straße 12, 04109 Leipzig, Germany
Full list of author information is available at the end of the article

provision and cooperation of information systems, missing solutions in terms of data security are inhibiting the broad utilization of this technology in businesses.

Especially smaller and medium-sized companies are on the one hand interested in the use of cloud systems [2]; on the other hand they are afraid of using them since they show insufficient informational right to say in terms of storage location and legal security [11], and they are afraid of the "lock-in effects" [2] of external-hosted utilization. Further, new and unsolved challenges concerning data security arise because of the possibility for the collection and analysis of big, distributed data files, i.e., in terms of the "Big Data Context" [12]. Key provisions for data security are defined in the German privacy laws and are therefore an informational self-rule but those laws are only applicable to private individuals and hence not suitable for a reliable protection of business data. Service providers from non-EU countries do not fulfil these requirements and are therefore not suitable for reliable data protection. Consequently, solution approaches, which guarantee the fulfillment of data protection regulations on an organizational and professional level during the operation of the information systems and during the transfer of data between the information systems, are needed.

Our central and design-orientated research issue results from this motivation:

How must a cloud-based ecosystem for the integration of decentralized information systems be built technologically and in terms of organization, in order to guarantee cloud user their privacy laws? To answer this question, we base our method on the "Heuristical Theorizing" research approach [13]. In order to structure our problem, we analyzed solution concepts for the organization of cloud ecosystems from the application area of social networks via a system comparison. Following on that, we developed requirements for the support of decentralized systems through literature research. Derived from the results, various organizational levels for a division of roles in cloud-based ecosystems were developed. The research artifacts are summarized in the following contribution. In the next step, a first conceptual architecture draft and a technical proof-of-concept prototype based on the results is developed. The evaluation proceeds according to the quick-and-simple strategy of the FEDS framework [14].

The article is structured as follows: In section 2 basic terms are explained. In section 3 the system comparison is described. In section 4 the results of our literature research, from which the catalog of requirements is derived, are summarized. Section 5 shows basic forms of organizational decentralization derived from the system comparison and the catalog of requirements. In section 6 the results are discussed and the following steps are shown. The article closes with the summary in section 7.

Basic terms

In the following, the terms "decentralized information systems" and "cloud systems" are classified with regard to the development of decentralized cloud ecosystems.

Data security peculiarities in these systems are described afterwards. The term "information system" describes a socio-technical man-machine system, which embeds itself into the organizational, personnel and technical structures of an institution [15]. The system can be categorized fully through five characteristic features: human, user properties, operational tasks, technology, and information behavior phases [16]. Decentralized information systems extend the term "information system" since they include aspects of a decentralization of stakeholder groups, technological components, and process cycles beyond company boundaries.

Decentralization can't be reduced down to the distribution of technological resources within an infrastructure. Organizational decentralization means externalization of responsibilities, rights, and duties within a superordinate process. Technological decentralization describes the use of distributed systems and the externalization of software system components. Both ways of decentralization are strongly connected, changing dynamically, and can influence each other. Because of the complexity of the decentralized structures and relations, the openness, and dynamic of the changing value-added structures, information systems can also be called ecosystems [17].

The term "cloud system" describes a network-based computer system, which can be used for organizational and technological integration into decentralized information systems, based on cloud computing technology. Applications and data are loosely connected, they communicate via network, and translate organizational distributed business processes. Because of open interfaces and dynamic composition, a reconfiguration of the system is possible. Technological decentralization based on distributed applications has to be considered as a requirement of organizational decentralization.

Organization of rights, duties and tasks for data security represents a central component of information systems, and the same is true for cloud (eco-) systems. The aim is to protect user data from unauthorized access, transfer and commercialization by third parties. With today's authentication technologies, authorization technologies and encryption technologies, communication and protection from unauthorized data access can be guaranteed, but looking at it from an organizational view, the problem concerning data security cannot be solved. Here, control over data of the cloud services provider, or rather cooperation partner, lies with the recipient. Therefore, a decentralized data keeping in cloud systems has to make it possible for all parties to decide on their own which data security regulations apply to their own data. Their adherence has to be transparent and controllable. The cloud system has to be designed so that changing data access regulations can be determined by the cloud user. Further, technological requirements and country-specific laws as well as "aspects of trust" have to be able to be integrated into the data access management and data access rights management. Data security principles such as "a specific purpose", "transparency", and "reliability of data generation and processing" apply to decentralized cloud systems, too [18]. It was shown that a decentralization makes an increasing adherence to data security requirements possible since control over data and applications is transferred to the user [10, 19]. Deriving from this motivation, forms and gradations of decentralization and its suitability for fulfilling requirements beyond data security have to be analyzed.

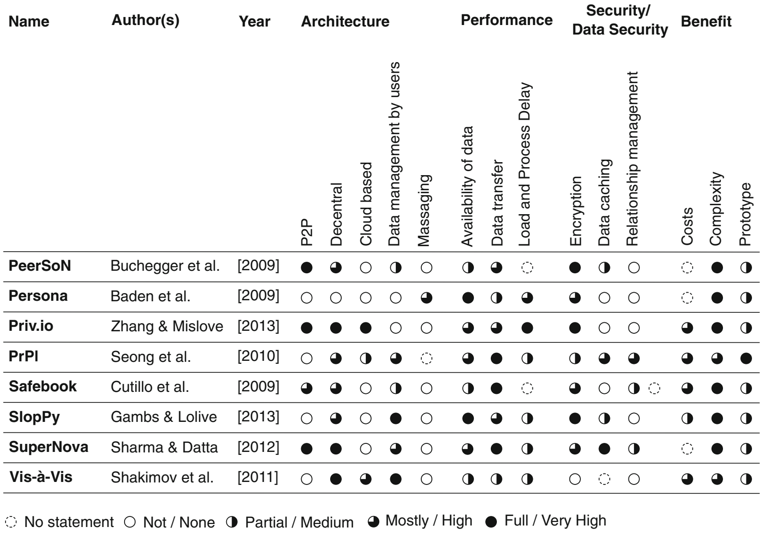
System comparison

We carried out a system comparison in order to structure the problem and to identify the established solution approaches for the organization of cloud ecosystems.

The field of research of decentralized organized social networks is very suitable for this comparison since decentralized cloud systems are already widely spread in this field and the topic data security is of high significance. Further, various references already exist and can be used as a comparable object.

The system comparison includes eight social network concepts in total. These eight concepts were analyzed in terms of architecture, performance, security/data security, and benefit. The results of the comparison are summarized in Fig. 1. The solutions of the investigated concepts of PeerSoN [20], Priv.io [21], Safebook [22], and SuperNova [23] are based on a peer-to-peer approach. The concepts PrPl [24], SlopPy [25], and Vis-à-Vis [26] are based on distributed applications and on server solutions as well as cloud solutions that are self-managed by the user. As a common ground of these concepts, all parties are expected to run and manage their own cloud system. The eight already mentioned systems will now be explained shortly and examined with regard to their currently unsolved problems.

PeerSoN by Buchegger et al. [20] is a peer-to-peer approach that focuses on privacy. In order to protect user data, encryption following the public-key-method is used. Thus, data can only be accessed with the right key. In general, all data is stored on the respective local computer of the users. A lookup service helps finding users and with the interaction. If a user is not online, data cannot be updated. The problem of limited data availability can be solved by storing data temporarily on a friend's computer. This, however, affects the data security negatively. Direct communication takes place via external applications. **Persona** by Baden et al. [27] is a solution approach that uses a central storage service. Further, it uses attribute-based encryption with fine granular rules. With the help of a browser extension, it can be integrated into an already existing SNS. However, first performance measurements showed that loading a big amount of data can take relatively long (up to 10 s). **Priv.io** by Zhang and Mislove [21] is a cloud-based approach. For this, two components, i.e., priv.io core and priv.io applications, were developed. Priv.io core is a Java application, which allows to access and manipulate user data. In addition, it is used for communication with other users. Priv.io applications allow the usage of further applications in this ecosystem. In general, Priv.io uses attribute-based encryption. The Priv.io application



Name	Author(s)	Year	Architecture					Performance			Security/ Data Security			Benefit		
			P2P	Decentral	Cloud based	Data management by users	Massaging	Availability of data	Data transfer	Load and Process Delay	Encryption	Data caching	Relationship management	Costs	Complexity	Prototype
PeerSoN	Buchegger et al.	[2009]	●	◕	○	◑	○	◑	◕	◌	●	◑	○	◌	●	◑
Persona	Baden et al.	[2009]	○	○	○	○	◕	●	◑	◕	◕	○	○	◌	●	◑
Priv.io	Zhang & Mislove	[2013]	●	●	●	○	○	◕	◕	●	●	○	○	◕	●	◑
PrPl	Seong et al.	[2010]	○	◕	◑	◕	◌	◕	●	◑	◑	◕	◕	◕	◕	●
Safebook	Cutillo et al.	[2009]	◕	◕	○	◑	○	◑	●	◌	◕	○	◑ ◌	◕	●	◑
SlopPy	Gambs & Lolive	[2013]	○	◕	○	●	○	●	◕	◑	●	◑	○	◑	●	◑
SuperNova	Sharma & Datta	[2012]	●	●	○	◕	○	◕	●	◑	◕	●	◑	◌	●	◑
Vis-à-Vis	Shakimov et al.	[2011]	○	●	◕	●	○	◑	◑	◑	○	◌	○	◕	◕	◑

◌ No statement ○ Not / None ◑ Partial / Medium ◕ Mostly / High ● Full / Very High

Fig. 1 Results of the degree of the fulfillment of the system comparison characteristics

has to be able to run on every cloud as a web service. All data is stored by the cloud provider. Therewith, data availability is guaranteed and costs rise. **PrPl** by Seong et al. [24] introduces a software component named Personal Cloud Butler. It is operated by the user himself or provided by another provider. Therewith, various data security levels arise, depending on who operates the software. Different instances of the Butler communicate with each other in order to build a network. Further, it is possible to add data from other systems (e.g., from Facebook). This concept is mainly organized in a decentralized way since each instance has to be set up by a user without having a central unit. **Safebook** by Cutillo et al. [22] is a decentralization approach with Real-life trust. Here, the aim was to solve the problem of trust between users, the system and its operators. Like many other solution concepts, P2P technology is used for communication and the development of the network. The connection is implemented via a Matryoshka architecture, which checks the trust between the users. Communication is set up through a social network server. **SlopPy** by Gambs and Lolive [25] is an approach for storing encrypted data on so-called semi-trusted instances. Here, data is transferred to friends but can only be accessed with the right key. The communication takes place via an anonymous communication network. Here, the problem of low availability is addressed. **SuperNova** by Sharma and Datta [23] is a P2P solution approach with Super-Peers. In this approach, friends store data for higher availability. So-called Storekeepers hold key tasks and keep the network running. **Vis-à-Vis** by Shakimov et al. [26] is an extensive concept of a decentral cloud-based social network. Virtual Individual Servers (VIS) are operated by the user himself or rented from a cloud provider. These VISs consist of a storage layer and a processing layer, which communicate. That way, user data can be exchanged. The system is local- and group-based and can be compared to Diaspora*.

All network concepts either fully or partly implement data accessibility and transaction encryption. Further, absolute decentralization without gradation is required. Often, the need of the user for simple operations is not the focus of the approach [28].

From comparison it can be seen that already-existing solution approaches prefer peer-to-peer as a technological realization since it isn't necessary to trust in a centralized authority and moreover, data security requirements can be applied. Challenges arise especially in terms of accessibility of data in these approaches. Further, it can be seen that a decentralization solution is more complex in terms of application compared to a centralized solution. Data transfer is comparatively high in all solutions and the time for the transfer is likely to increase when the number of users increases.

Requirements analysis

In addition to the comparison of the system and for further structuring, we conducted a systematic literature research from which we derived requirements for the design of a cloud ecosystem that followed data security laws. The literature research was conducted in international A+, A and B information system journals, i.e., Information Systems Research, Management Information Systems Quarterly and Journal of Management Information Systems, based on the VHB ranking [29]. After following the method according to Denyer [30], a keyword search within the context of decentralization, information systems, and data security was used. Following that, titles and abstracts were selected. Ultimately, insights and requirements for the design of information systems were gained through extraction and synthesis.

Altogether, 14 contributions with a high relation to the topic were identified. Afterwards, 21 recommendations for the conception of data security in decentralized cloud systems were taken from these contributions. We then assigned these recommendations through content structuring to the fields of data security, trust, relationship management, and system design. All requirements were evaluated and adapted according to quality criteria. According to Pohl [31], quality criteria are: completeness, transparency, correctness, clarity, understandability, consistency, controllability, evaluation, topicality, and atomicity. That way, it was possible to identify unspecified issues and to correct them in a targeted way. These requirements were completed by six further requirements, which were taken from the results of the system comparison and the information of the relevant authors. The first catalog of requirements consists of 27 requirements and is summarized in Table 1.

"Basic system requirements" describes basic requirements for future conceptions.

It becomes clear that a central authority, so-called "Trusted Party", represents an especially expedient solution approach [32]. However, this means that a first restriction concerning decentralization takes place since a jointly agreed on neutral and trustworthy authority is now needed. Further, it should still be the aim to make preferably low costs possible and to use already-existing offers at the current market.

That way, through a distribution of service provisions and the respective specialization of service providers, a high-quality overall offer is created. External user data storage can be mentioned as an example. Additionally, an all-inclusive new development can be avoided. An alternative level of data security can be adapted, aimed at various target groups for future participants [33, 34]. When using external resources, it is necessary to ensure availability as far as possible [35].

"Data security" sets a special focus on data security aspects and their application within information systems.

Table 1 Catalogue of requirements

ID	Description
CO	Basic system requirements
CO1	System as central authority of trust ("Trusted Party")
CO2	Use of services offered at the market, which need little user configuration
CO3	Basic use of system without user costs
CO4	Alternative selection of data security level
CO5	Provide possibility for data encryption on storage medium
CO6	Integration of user management
CO7	Complete availability of necessary resources in the form of data
DS	Data Security
DS1	Data security has to be highlighted visually for the user
DS2	Control over data usage with an option for (automatic) deletion
DS3	Simple rights management to avoid conflicts
DS4	User anonymity within the system
DS5	Personal data protection through user or authority for data management
DS6	Attached protection policies for data
DS7	Co-data security for jointly created user data (Co-Privacy)
DS8	Recommendation for data security settings
TR	Trust
TR1	Centralization of trust
TR2	Creation of trust of the user (i.e., via support from other user)
RM	Relationship Management
RM1	Support for contact management
RM2	Automatic derivation of relations
SY	System Design
SY1	High number of data sources through a high abstraction of the access layer
SY2	Concept for the availability and non-availability of user data
SY3	System robustness against attacks and incorrect data
SY4	Fine granular
SY5	Inoperability
SY6	Rights and interaction management based on relationships
SY7	High-performance search within the network
SY8	Self-presentation management (monitoring/feedback)

Basically, what is needed is all-inclusive data security control, involving high transparency and understandability for the user [36]. A simple rights management helps the user when defining rules. Through low complexity, better implementation and a reduction of wrong decisions are made possible [37]. To delete unused data, the system has to work automatically and in a transparent way for the user [38]. Attached protection policies, i.e., in form of meta data, assist when allocating data and make a theoretical transfer into another system possible [39]. Nowadays, data cannot only be assigned to one user because they consist of many different parts. Hence, it must be made possible that the so-called Co-Privacy is displayed and implemented conceptually in an information system [39].

The sector "Trust" explicitly requires decentralizing the Co-Privacy. Further, it is pointed out that trust has to be created, i.e., via other user [40]. For this, the relationship management has to be created. The management has to be able to automatically derive relations [39, 41].

The sector "system design" sets basic requirements for the system. Here, fine granularity, robustness, and interoperability are basic elements. Monitoring and feedback are helping the user when using the system. The high number of sources for external data represents the openness of the system [35, 39].

Organizational levels analysis

Various organizational levels for a division of roles in terms of data security in cloud (eco-) system can be derived from the system comparison and requirements analysis. Here, parties involved can act in different roles: infrastructure provider, user of infrastructure, or both. Moreover, trust toward other participants is extremely important—especially when talking about a high decentralization. This means new concepts of trust are needed and the situation can't be handled without the inclusion of the environment. Consequently, the government, as the most trustworthy authority, is to be involved in the consideration, acting within the legal framework. Based on these insights, an organizational model was created, which represents a network-of-relationships model of the various parties. All parties involved have different requirements and aims for the network, hence different forms of relationship constellations arise. Figure 2 summarizes the various forms of organizational decentralization.

Following, levels of organizational decentralization are explained. The model of organizational decentralization is divided into five stages, whereas the first stage (Level 0: None (Central)) doesn't contain any decentralization aspects. These levels correspond to the currently most common solution approach where all customer data is stored centrally. The shift to the next level represents another organizational structure.

Already existing system implementations and system approaches can be assigned to exactly one level. The higher the level, the higher the decentralization.

Level 0: Centralized

Level 0 is characterized by completely centrally organized applications and a range of services. Most recent

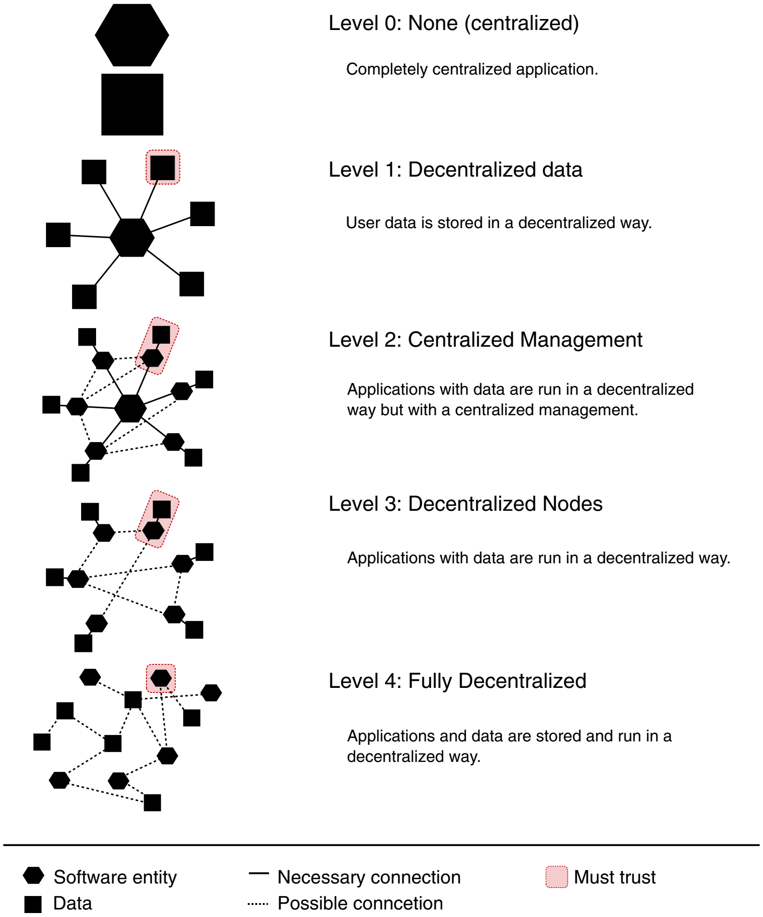

Level 0: None (centralized)
Completely centralized application.
Level 1: Decentralized data
User data is stored in a decentralized way.
Level 2: Centralized Management
Applications with data are run in a decentralized way but with a centralized management.
Level 3: Decentralized Nodes
Applications with data are run in a decentralized way.
Level 4: Fully Decentralized
Applications and data are stored and run in a decentralized way.
Software entity
Data
Necessary connection
Possible conncetion
Must trust

Fig. 2 Overview of organizational decentralization

Internet platforms can be assigned to this level. This is due to the fact that the creation of service offers can take place independent from the participants. Hence, it is possible to implement a system in a simple way without restrictions.

Another advantage for companies is that data can be kept as an economic asset within the application. Following this concept, responsibilities, rights, and duties do not have to be transferred to a third party. Participants need to trust the provider completely. This is being criticized by many customers at the moment [42].

Level 1: Decentralized data

On Level 1, a decentralization in terms of externalization of user data takes place. The cloud computing technology called “Storage Cloud” is suitable for the technological implementation since it enables an easy integration of data storage of user into the system. The centrally acting provider takes the roles of trustworthy authority and data management without storing any user data on their own. Complete trust dissolves partially and user takes on more rights and duties. For a high-quality range of services, a guarantee of data availability is essential.

Level 2: Centralized management

Level 2 is characterized by the relocation of applications and data to the participants and a centralized management. In many systems, a centralized Registry is used for the connection of the nodes in order to connect the participants with each other. The service-orientated paradigm is a typical example of this kind of organizational form. Further, the concept is implemented in the World Wide Web. The so-called “Domain Name” server redirects centralized-managed web addresses to the server. Here, it has to be considered that the centralized management needs to be trusted in terms of identity checks of the participants.

Level 3: Decentralized nodes

On Level 3, a centralized management of the network is missing so the participants need to organize the cooperation and interaction on their own. In the field of social networks, Diaspora* [43] is a representative that supports this concept. It has to be mentioned that self-managed nodes can raise difficulties for persons without technological knowledge. Basically, the principle follows the peer-to-peer approach. Some approaches use the principle of distributing data to various participants in order to achieve high-availability.

Level 4: Fully decentralized

The last stage, Level 4, describes a full decentralization of all components, meaning that data and applications are being stored and run separately. This concept can be found in the field of "Internet of Things" [7] and in the "Fog Computing-Paradigma" [10]. Currently, the implementation of this stage is subject to recent research. What's striking is that only the whole ecosystem needs to be trusted but not the centralized provider. Future research has to investigate if such a concept can work without a centralized management.

All described stages can be operated and implemented with various forms of technological decentralization. Hence, this is a clearly organizational model. For the evaluation of the introduced model, systems and concepts are being assigned to the respective levels. A falsification is displayed if a system can't be assigned to a level.

Results discussion and next steps

The results discussion is divided according to the presented artifacts of the analysis phase into the section "requirements catalog" and "organizational decentralization model."

The requirements catalog introduced in this contribution brings together insights from research and presents guidelines for a conceptualization of ecosystems with decentralized organized information systems. The primary criterion is the creation of trust between all members of the network (see: CO1). Therefore, extensive analysis of solution strategies regarding legal and technological aspects are needed. Since it was shown that the centralization of trust is the most successful variant, a peer-to-peer solution, as introduced in other concepts, is to be excluded completely. That way, a wide range of variants of possible system concepts is restricted implicitly. New insights coming from research and experience make it necessary to extend or rather adapt the collected requirements accordingly. Further, it has to be analyzed if all requirements can be realized within a system entirely. Here, a prototypical implementation of all requirements serves as the basis for an evaluation. The application of already existing solutions on the market (see: CO2) applies mainly to external data storage. The integration of many sources is very complex. Especially a full availability of resources (see: CO7) requires strategies in case of non-availability (see: SY2). Basically, the aim is to gain more control over personal data. In order to involve user more, a storage cloud solution is offered. For the user, this means additional expenses and giving away responsibility. Based on this, a first concept idea is seen in Fig. 3.

The organizational decentralization model is the first step toward a classification of roles and the increase of trust toward cloud ecosystems. For the evaluation of the developed model, already existing concepts and approaches from the current research were classified. The classification of the introduced systems into the model of organizational decentralization is split into a complete application sovereignty and data sovereignty, and into the usage of a central management. Safebook, and SuperNova can be assigned to Level 2. PeerSoN, Priv.io, PrPl, SlopPy und Vis-à-Vis do not need a central management and can therewith be assigned to Level 3. In case of falsification, new concepts have to be developed, which cannot be assigned to any level. Then, the model will be extended or adapted.

While categorizing systems, it could be seen that Level 1 (Decentralized Data) was not represented. The distribution of data, i.e., distributed in data bases, is a strategy used in practice in order to deposit data. It was seen that this kind of strategy does not occur in a relational context. Further, it was seen that there is a connection between the increase of decentralization and the decrease of necessary trust toward other participants. Hence, Level 0 provides absolute trust in the provider. In practice, trust in large providers is lost so other solution approaches try to reduce the necessary trust. Altogether, it was seen that in practice and with the current service range of Internet services, Level 0 is being used the most. To some extent, this is due to the fact that complexity of software application development increases to the same extent as decentralization. Concerning loosely-linked components, further increase of data transmission is expected.

In order to answer the presented questions, future research needs to choose a level of organizational decentralization and to implement this level into an exemplary information system. Challenges for all decentralized architectures are the fields of data security and availability. Further, a trustworthy authority (Trusted Party) needs to be installed while considering and analyzing all local circumstances concerning data security

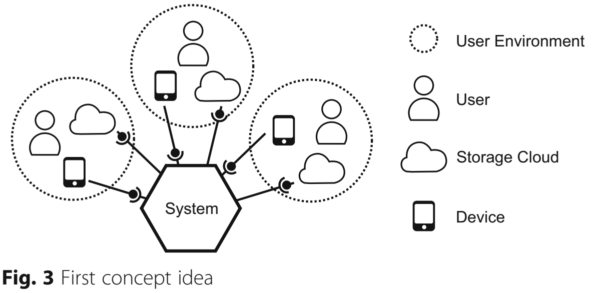


Fig. 3 First concept idea

guidelines and legislation. Therefore, the next research step consists of implementing a Proof-of-Principle and, following on that, a Proof-of-Concept prototype. The aim is to develop a system with low complexity and at the same time high data security. Here, the user needs to answer questions concerning the decrease of complexity and the increase of data security and acceptance.

Conclusion

This contribution introduced *research artifacts* in order to answer our research issue: *How must a cloud-based ecosystem for the integration of decentralized information systems be built technologically and in terms of organization, in order to guarantee cloud users their privacy laws?* In order to structure the problem, a system comparison from the field of social networks was carried out, and basic forms of the organization of cloud systems were analyzed. It became clear that peer-to-peer approaches as technological realization are favored since they do not require trust toward the centralized authority. Additionally, the users need to run their own systems. From the then conducted literature analysis, 27 requirements for the implementation of decentralized systems with the focus on data security were raised. It was shown that trust is a key element when it comes to data security aims and that users are becoming more involved in the process of creating services. Finally, various organizational levels for a division of roles in cloud-based ecosystems were introduced. The presented model can be used for the application of already existing concepts and as a support for the conceptualization of new approaches.

Acknowledgements

We acknowledge support from the German Research Foundation (DFG) and Universität Leipzig within the program of Open Access Publishing.

Authors' contributions

AM and AL carried out the literature review and the system comparison. AM did the requirements analysis and organizational levels analysis. AL introduced the FEDS framework for evaluation and was mainly part of the results discussion. BF provided useful insights and guidance and critically reviewed the manuscript. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Author details

[1]Department of Business Information Systems, Leipzig University, Grimmaische Straße 12, 04109 Leipzig, Germany. [2]Kühne Logistics University, Großer Grasbrook 17, 20457 Hamburg, Germany.

Received: 8 March 2017 Accepted: 18 May 2017
Published online: 28 June 2017

References

1. Statista (2015) Einsatz von Cloud Computing in deutschen Unternehmen bis 2015 Umfrage Statista, http://de.statista.com/statistik/daten/studie/177484/umfrage/einsatz-von-cloud-computing-in-deutschen-unternehmen-2011/. Accessed 18 Aug 2016
2. IDC (2015) IDC Studie: Hybrid Clouds nehmen angesichts der Digitalen Transformation Fahrt auf in deutschen Unternehmen, http://idc.de/de/ueber-idc/press-center/63144-idc-studie-hybrid-clouds-nehmen-angesichts-der-digitalen-transformation-fahrt-auf-in-deutschen-unternehmen. Accessed 5 Aug 2016
3. BITKOM (2014) Wie Cloud Computing neue Geschäftsmodelle ermöglicht, https://www.bitkom.org/Publikationen/2014/Leitfaden/Wie-Cloud-Computing-neue-Geschaeftsmodelle-ermoeglicht/140203-Wie-Cloud-Computing-neue-Geschaeftsmodelle-ermoeglicht.pdf. Accessed 18 Aug 2016
4. Ropohl G (2009) Allgemeine Technologie. Eine Systemtheorie der Technik. Universität Karlsruhe Universitätsbibliothek, Karlsruhe
5. BMBF: Die neue Hightech-Strategie: Innovationen für Deutschland (2014)
6. BMWi, BMI, BMVI: Digitale Agenda 2014–2017. München (2014)
7. Atzori L, Iera A, Morabito G (2010) The Internet of Things: A survey. Comput Netw 54:2787–2805
8. Beetz K (2010) Die Wirtschaftliche Bedeutung von Cyberphysical Systems aus der Sicht Eines Global Players. In: Broy M (ed) Cyber-Physical Systems. Springer, Berlin Heidelberg, pp 59–66
9. Software-Cluster (2015) Emergente Software, http://www.software-cluster.com/de/forschung/themen/emergente-software. Accessed 24 Nov 2015
10. Vaquero LM, Rodero-Merino L (2014) Finding Your Way in the Fog: Towards a Comprehensive Definition of Fog Computing. SIGCOMM Comput Commun Rev 44:27–32
11. TecChannel (2014) Cloud Computing - der deutsche Mittelstand hinkt hinterher - TecChannel-Studie TecChannel.de, http://www.tecchannel.de/wege_in_die_cloud/2053924/cloud_studie_tc_2014_tx/index.html. Accessed 29 Jan 2016
12. Smith M, Szongott C, Henne B, Voigt Gv (2012) Big data privacy issues in public social media. In: 2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST), pp 1–6
13. Gregory RW, Muntermann J (2014) Research Note—Heuristic Theorizing: Proactively Generating Design Theories. Inf Syst Res 25:639–653
14. Venable J, Pries-Heje J, Baskerville R (2014) FEDS: a Framework for Evaluation in Design Science Research. Eur J Inf Syst 25:77–89
15. Laudon K.C, Laudon J.P, Schoder D (2009) Wirtschaftsinformatik: Eine Einführung. Pearson Studium, München
16. Heinrich L.J, Heinzl A, Riedl R (2010) Wirtschaftsinformatik: Einführung und Grundlegung. Springer, Berlin
17. Moore JF (1997) The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems. Harper Paperbacks, New York
18. Erklärung von Montreux: Ein universelles Recht auf den Schutz personenbezogener Daten und der Privatsphäre unter Beachtung der Vielfalt in einer globalisierten Welt. 27. Internationale Datenschutzkonferenz in Montreux, Montreux (2005)
19. Yeung C-MA, Liccardi I, Lu K, Seneviratne O, Berners-lee T (2009) Decentralization: The future of online social networking. In: In W3C Workshop on the Future of Social Networking Position Papers
20. Buchegger S, Schiöberg D, Vu L-H, Datta A (2009) PeerSoN: P2P Social Networking: Early Experiences and Insights. In: Proceedings of the Second ACM EuroSys WS on Social Network Systems. ACM, New York, pp 46–52
21. Zhang L, Mislove A (2013) Building Confederated Web-based Services with Priv.Io. In: Proceedings of the First ACM Conference on Online Social Networks. ACM, New York, pp 189–200
22. Cutillo LA, Molva R, Strufe T (2009) Safebook: A privacy-preserving online social network leveraging on real-life trust. IEEE Commun Mag 47:94–101
23. Sharma R, Datta A (2012) SuperNova: Super-peers based architecture for decentralized online social networks. In: 2012 Fourth International Conference on Communication Systems and Networks (COMSNETS), pp 1–10
24. Seong S-W, Seo J, Nasielski M, Sengupta D, Hangal S, Teh SK, Chu R, Dodson B, Lam MS (2010) PrPl: A Decentralized Social Networking Infrastructure. In: Proceedings of the 1st ACM 2010, pp 8:1–8:8

25. Gambs S, Lolive J (2013) SlopPy: Slope One with Privacy. In: Di Pietro R, Herranz J, Damiani E, State R (eds) Data Privacy Management and Autonomous Spontaneous Security. Springer, Berlin Heidelberg, pp 104–117
26. Shakimov A, Lim H, Caceres R, Cox LP, Li K, Liu D, Varshavsky A (2011) Vis-à-Vis: Privacy-preserving online social networking via Virtual Individual Servers. In: 2011 Third International Conference on Communication Systems and Networks (COMSNETS), pp 1–10
27. Baden R, Bender A, Spring N et al (2009) Persona: An Online Social Network with User-defined Privacy. Proceedings of the ACM SIGCOMM 2009 Conference on Data Communication. ACM (SIGCOMM '09), New York, pp 135–146. doi:10.1145/1592568.1592585. ISBN: 978–1–60558-594-9
28. Narayanan, A., Toubiana, V., Barocas, S., Nissenbaum, H., Boneh, D.: A Critical Look at Decentralized Personal Data Architectures. arXiv:1202.4503 [cs] (2012)
29. VHB (2015) Teilrating WI: Verband der Hochschullehrer für Betriebswirtschaft e.V, http://vhbonline.org/service/jourqual/vhb-jourqual-3/teilrating-wi/. Accessed 19 Nov 2015
30. Denyer D (2013) Doing a literature review in business and management, http://www.ifm.eng.cam.ac.uk/uploads/Research/RCDP/Resources/Working_with_literature_for_Cambridge.pdf. Accessed 19 Nov 2015
31. Pohl K (2008) Requirements Engineering: Grundlagen, Prinzipien,Techniken. dpunkt.Verlag GmbH, Heidelberg
32. Sarker S, Ahuja M, Sarker S, Kirkeby S (2011) The Role of Communication and Trust in Global Virtual Teams: A Social Network Perspective. J Manag Inf Syst 28:273–310
33. Williams P, Sion R (2013) Access Privacy and Correctness on Untrusted Storage. ACM Trans Inf Syst Secur 16, 12:1–12:29
34. Erway CC, Küpçü A, Papamanthou C, Tamassia R (2015) Dynamic Provable Data Possession. ACM Trans Inf Syst Secur 17, 15:1–15:29
35. Tigelaar AS, Hiemstra D, Trieschnigg D (2012) Peer-to-Peer Information Retrieval: An Overview. ACM Trans Inf Syst 30, 9:1–9:34
36. Tsai JY, Egelman S, Cranor L, Acquisti A (2011) The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. Inf Syst Res 22: 254–268
37. Ni Q, Bertino E, Lobo J, Brodie C, Karat C-M, Karat J, Trombeta A (2010) Privacy-aware Role-based Access Control. ACM Trans Inf Syst Secur 13, 24:1–24:31
38. Karla J (2010) Can Web 2.0 Ever Forget? Bus Inf Syst Eng 2:105–107
39. Fogues R, Such JM, Espinosa A, Garcia-Fornes A (2015) Open Challenges in Relationship-Based Privacy Mechanisms for Social Network Services. Int J Hum Comput Interact 31:350–370
40. Liu D, Brass D, Lu Y, Chen D (2015) Friendships in Online Peer-to-Peer Lending: Pipes, Prisms, and Relational Herding. Manag Inf Syst Q 39:729–742
41. Davison RM, Ou CXJ, Martinsons MG (2013) Information technology to support informal knowledge sharing. Inf Syst J 23:89–109
42. IfD, glh, Institut für Demoskopie Allensbach, Centrum für Strategie und Höhere Führung: Cyber Security Report 2015: Ergebnisse einer repräsentativen Befragung (2015)
43. diaspora* (2016) Über - Das Projekt diaspora*, https://diasporafoundation.org/about. Accessed 25 Aug 2016