Trust as an Integral Part for Success of Cloud Computing

Felix Meixner, Ricardo Buettner
FOM Hochschule fuer Oekonomie & Management, University of Applied Sciences
Chair of Information Systems, Organizational Behavior and Human Resource Management
Arnulfstrasse 30, 80335 Munich, Germany
f.meixner@ieee.org, ricardo.buettner@fom.de

***Abstract*—Cloud computing has become a hot topic in research in the enterprise and consumer sector. It is clear to everyone that the opportunities and applications of cloud computing are versatile and that cloud computing is an emerging computing paradigm. However when decisions on adopting cloud computing-related solutions are made, trust and security are two of the most critical obstacles for the adoption and growth of cloud computing today. We think there are ways to largely eliminate concerns of potential cloud users by taking advantage of numerous existing technological possibilities, including trust-building measures, like standardization, cryptography, isolation and many more.**

Keywords-cloud computing; security; identity-management; encryption; trust

I. INTRODUCTION

Cloud Computing can be regarded as the most important evolution of the mid 1990's concept of grid computing [1]. In recent years cloud computing clearly became the trend to follow in the IT-industry, providing flexible and scalable software-, platform- and infrastructure-services on demand [2]. However, to fully leverage its potential for cost-savings, cloud computing still has to overcome some major obstacles. As traditional network borders are breaking down at the same time as security threats are increasing, the most important concern about cloud computing are issues of security and trust that have only been partially solved so far.

A lot of literature about cloud computing, trust and security does exist, though most of it is IT-centric [3] [4] [5] [6]. What is less examined and documented is the human perspective that examines the shortcomings of cloud computing, people's expectations and anxieties as well as psychological aspects. This paper's objective is to focus on both perspectives, IT and human and try to narrow the gap between both by offering a state of the art overview of mechanisms that help secure the use of cloud computing and thereby create trust in cloud computing. The research question is: Can cloud computing gain enough trust from its users and customers to be even more successful and become an indispensable utility like the power grid?

Our approach to this subject included research on the history and state of cloud computing today, thereby identifying trust and security as the most critical factors of success for future growth and adoption. With these findings in mind, our research was refined on trust and security in cloud computing and its supporting and control mechanisms. The research methodology included investigating multiple of the most relevant online scientific journals databases (Springer Link, JSTOR, ScienceDirect, Elsevier, IEEE Xplore Digital Library and ACM Digital Library).

The remainder of the paper is organized as follows: In Section II we recognize related work. Then the paper gives an insight into the history, different types and sources of trust in non-technological fields and ways in Section III. These fields include trust in general, in psychological and in economical aspects. The paper outlines the difference between party trust and control trust and sets up a framework for trust that is transferred to Section IV, where the framework is mapped to cloud computing technology. The paper continues with Section V by describing various types of technology aiming to enhance user's and decision makers trust in cloud computing. Finally, in Section VI, we draw the conclusion and provide recommendations for future work and show the need for optimizing existing trust infrastructure and mechanisms.

II. RELATED WORK

In his article "Cloud Computing", Brian Hayes discusses the trend of moving software applications into the cloud and the related trust privacy, security, and reliability challenges [7]. E. Pearson focuses on privacy challenges as important issues for cloud computing, both in terms of legal compliance and user trust and says that it needs to be considered at every phase of design. He suggests key design principles for software engineers and argues that privacy must be considered when designing any aspects of cloud services, for both legal compliance and user acceptance [8]. The article "A View of Cloud Computing" defines classes of utility and cloud computing and creates a ranked list of critical obstacles to adoption and growth of cloud computing. The list includes availability, data lock-in, data confidentiality and auditability as the top three factors for adoption [9]. M. Mowbray and S. Pearson of HP Labs in their paper "A Client-Based Privacy

 ISBN: 978-1-61208-200-4

Manager for Cloud Computing" state that processing sensitive user data in the cloud poses a significant barrier to the adoption of cloud services and that users fear data leakage and loss of privacy. Mowbray and Pearson describe a client-based privacy manager that helps reduce this risk as well as providing additional privacy-related benefits by reducing the amount of sensitive information sent to the cloud [10].

III. CONCEPTS, TYPES AND SOURCES OF TRUST

People have been aware of the concept of trust for quite a long time. In fact, it is as old as the history of man and the existence of human social interactions [11]. The majority of literature and studies about trust comes from classic disciplines like philosophy, psychology and economics, all of which concentrate on exploring a general understanding of trust. This paper focuses on trust in cloud computing, by referring to these studies that explain classic forms of trust alias offline trust.

Philosophy traces the concept of trust back to the ancient Greek. They believed that people trusted others, only if they were confident that the others feared detection and punishment enough to deter them from harming or stealing.

Psychology focuses on interpersonal trust and agrees that it was an especially important concept in psychology and vital to personality development (Erikson, 1963) [12], cooperation institution (Deutsch, 1962) [13] and social life (Rotter, 1980) [14]. Rotter gave a frequently cited definition of interpersonal trust as "an expectancy held by individuals or groups that the word, promise, verbal, or written statement for another can be relied on [14]." He has also proven through experiments, that trust has positive consequences to people and society overall.

Economics study trust intensively in organizational contexts. Among other factors it is considered a predictor of satisfaction in organizational decision-making. It was also recognized that trust is able to reduce the cost of both intra- and inter-organizational transactions and able to enhance business performance [15]. Trust, defined as "a willingness to rely on an exchange partner in whom one has confidence", assumed an essential role in establishing and maintaining a long-term relationship between sellers and customers [16].

It can be stated already, that trust is a complex, subjective and abstract concept that is difficult to define. You can find many definitions of trust in literature substituting it with credibility, reliability or confidence. The Oxford English Dictionary in 1971 defines trust as "confidence in or reliance on some quality or attribute of a person or thing, or the truth of a statement''. Mainly though it is a mechanism reducing social complexity on the one hand, but causing vulnerability towards something or somebody on the other hand.

In an article regarding e-commerce, Tan and Thoen considered party trust, control trust and the duality between trust and control as important concepts [17]. Party Trust means trust in the other party. It is subjective and has both an action and an information perspective. Mayer et al. define it as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other party will perform a particular action important to the truster, irrespective of the ability to monitor or control that other party [18]." Control Trust means the trust that is created by a control mechanism. It tends to be more objective than party trust. If there is not enough party trust in a situation, an instance of control trust should be used to increase the overall level of trust. For example, getting a receipt at the dry cleaners stating how many pieces of clothes you handed in, increases your level of trust to get all the pieces back later on.

Psychology was found to one of the most important aspects of trust, which is why it is helpful to have a framework of criteria on how trust is generally observed. Using this framework it will then be possible to draw comparisons between offline trust, in the before described sense, and online trust in the field of technology and cloud computing. According to the overview of Wang and Emurian [11] most researchers study four characteristics of trust:

1. Trustor and trustee

A trusting relationship always consists of a trusting party (trustor) and a party to be trusted (trustee). "The development of trust is based on the ability of the trustee to act in the best interest of the trustor and the degree of trust that the trustor places on the trustee"[11].

2. Vulnerability

The concept of trust only works and is needed in environments where vulnerability, uncertainty and risk are involved. A trustor relies on the trustee not to exploit his vulnerabilities.

3. Produced actions

"Trust leads to actions, mostly risk-taking behaviors. The form of the action depends on the situation, and the action may concern something either tangible or intangible [11]."

4. Subjective matter

In every case trust is a subjective matter. Each individual regards trust differently on a case-by-case basis being influenced by personal and situational factors.

IV. TRUST IN CLOUD COMPUTING TECHNOLOGY

As the introduction of the paper says, some of the major concerns in cloud computing are trust and security. Trust is one of the most critical obstacles for the adoption and growth of cloud computing. Therefore, in this section we will not only refer to the framework with the four characteristics of trust we have just laid out in the preceding chapter, but go beyond this and include security as an object of study, which interacts bilateral with trust.

1. Trustor and trustee

The cloud also relies heavily on the concept of trustor and trustee parties to establish trusting relationships. The difference is that with online trust, the distribution of roles is narrowed down to the cloud service provider being the trustee and the cloud service customer or end user being the trustor.

 ISBN: 978-1-61208-200-4

2. *Vulnerability*

The count of vulnerabilities enterprises face in cloud computing are innumerable. In the digital age of software bugs and ideological hacking groups such as "anonymous" and "LulzSec", the news are full of exploited vulnerabilities in the Internet. They reach from inadvertent loss of privacy and data theft, to loss of reputation and therefore money. Together, these reasons contribute to the necessity of trust in an insecure and hostile online world.

3. *Produced actions*

Customer's trust in cloud service providers can generate a couple of desired actions. An enterprise starts using a cloud service and shares its private and precious data with the cloud computing provider. On top of that, an enterprise might be confident to even pay for the cloud service and continue using it on a regular basis.

4. *Subjective matter*

Trust in cloud computing and technology is fundamentally as subjective as its offline counterpart. Again each individual and enterprise has different affections and preferences regarding technology that influences the level of trust towards cloud computing.

Meanwhile even more frameworks regarding trust in cloud computing exist. For example, a recent study from the University of Adelaide showed how to determine the credibility of trust feedbacks. In their paper "Trust as a Service: A Framework for Trust Management in Cloud Environments" they implement the Trust as a Service (TaaS) framework to improve ways on trust management in cloud environments [19].

V. CREATING SYSTEMIC TRUST THROUGH IT TECHNOLOGY

In a world wide web and in clouds of anonymity personal trust is a trait that is very hard to find. Therefore, cloud computing has to earn the trust of enterprises, decision makers and users, by relying on other forms of trust. Fortunately, there are many methods to create systemic trust by means of control mechanisms and help of modern virtualization and security technology.

The next sections follow and expand a proposal for a reference deployment model to eliminate user concerns on cloud security by Zhao, Rong, Jaatun and Sandnes [20]. The model deals with security related issues in cloud computing and proposes five service deployment models to address these issues. The proposed model provides different security related features to address different requirements and scenarios. While some scenarios of the deployment model have multiple valid solutions at hand, others have not yet been entirely solved. Keeping the model in mind it is used as a basis and expanded with some similar, but more practical solutions towards a trusted and secure enterprise cloud:

A. Separation, Isolation and Multi-Tenancy

B. Availability and Reliability

C. Data and Service Migration

D. Cryptography

E. Contractually Fixed Agreements

F. Certifications, Standards Compliance and IT Service Quality

G. Transparency

A. *Separation, Isolation and Multi Tenancy*

Some central mechanisms of increasing importance are identity management and access control. They fit into the category of separation, isolation and multi-tenancy. In contrast to applications and services hosted in-house, proper access management is a must-have. As soon as enterprises decide to use more than one cloud computing service, the challenge rises quickly, due to a couple of issues. Users have to deal with an inflation of credentials, thus increasing the risk of simple and re-used passwords for multiple services. The responsible IT-Managers cannot oversee the access rights of employees or users that are spread across multiple cloud service providers. This fact leads to difficulties in access control management, especially if changes in responsibilities or personnel take place, or an employee resigns. This decentralized identity management also makes central logging of access much more difficult.

A solution to this issue could be to recentralize identity management and access control back into the enterprise by means of single-credential and single-sign-on solutions. A single-credential solution uses a master identity store, either replicated to the cloud, or queried by the cloud service provider, for example via Lightweight Directory Access Protocol (LDAP). A Single-Sign-On solution leverages the single-credential solution and requests authentication from the user only once at the first login. Subsequent authentications to cloud services are automated via asymmetric encryption mechanisms such as Public Key Infrastructure (PKI) using the trust model of certificate authorities (CA). These underlying mechanisms are transparent to the user. Both solutions require an effective protection of the central identity store, as a theft of those credentials provides potential access to all cloud services, granting access based on single-credential or SSO solutions [21].

In their article "Isolation in Cloud Computing and Privacy-Enhancing Technologies" N. Sonehara, I. Echizen and S. Wohlgemuth discuss the common issues around data leakage and loss of privacy [22]. They see isolation as a special kind of privacy protection mechanism, which avoids information exchange between cloud services through their users. Furthermore, isolation should be able to hide the objectives of cloud-users from the cloud service provider. They agree with Ambrust et al. 2010 [9] that the most current and common security mechanism in today's clouds, to reach the goal of isolation, is primarily virtualization. Ambrust states "It is a powerful defense, and protects against most attempts by users to attack one another or the underlying cloud infrastructure. However, not all resources are virtualized and not all virtualization environments are bug-free. … Incorrect network virtualization may allow user code access to sensitive portions of the provider's infrastructure, or to the resources of other

 ISBN: 978-1-61208-200-4

users. These challenges, though, are similar to those involved in managing large non-cloud data centers, where different applications need to be protected from one another. Any large Internet service will need to ensure that a single security hole doesn't compromise everything else [9]." Due to such flaws in technology, it is important not only to rely on a single mechanism to provide trust and security, but to interlink and connect with other mechanisms, as explained in the following sections.

B. Availability and Reliability

Some of cloud computing's key requirements for information security are availability and reliability. Data centers and cloud services should be designed for scalability and performance as well, and limit the necessity of human interaction [23]. Nonetheless we have seen a number of complete datacenters outages in the recent past, including market leaders such as Amazon and Google. Undheim, Chilwan and Heegaard focus on four different types of failures, namely failures in the power distribution or cooling, network failures, management software failures and server failures [24]. For all types of potential failures there are mechanisms in place that help to reduce the availability- and reliability risks to a minimum level. Two of the four mentioned types of failures were picked, and related work was investigated:

Regarding network failures, Gill, Jain and Nagappan present a large-scale analysis of failures in a data center network [25]. Their key observations state that data center networks are already reliable, especially because of their highly redundant design. Nevertheless, there is room for improvement in some areas. They state that load balancer reliability and the effectiveness of network redundancy have to be improved to mask the impact of network failures from applications. Further they recommend separating the network control plane from the data plane to avoid undesirable interference between application and control traffic.

Venkatesh and Nagappan study server failures, hardware repairs and reliability for large cloud computing datacenters and present a detailed analysis of failure characteristics, as well as a preliminary analysis on failure predictors. They state that "8% of all servers can expect to see at least 1 hardware incident in a given year and that this number is higher for machines with lots of hard disks. … Chances of seeing another failure on the same server is high. We find that the distribution of successive failure on a machine fits an inverse curve. … We also find that the location of the datacenter and the manufacturer are the strongest indicators of failures, as opposed to age, configuration etc. [26]." In ongoing work they are working on models for server reliability, including replacing hard disk drives (HDD) with solid state drives (SDD) for better reliability.

Now that we have given an insight into various types of failures, we want to show a conceptual and simple solution design, to circumvent all types of failures that jeopardize availability and reliability of cloud services. The reference deployment model of Zhao, Rong, Jaatun and Sandnes [20] corresponds with the central point on Ambrust's [9] top ten list of obstacles for growth of cloud computing, namely availability + business continuity. Their solution is to use multiple cloud service providers, as they describe in their reference deployment model. The model builds an availability model on top of at the best already redundantly designed cloud infrastructure, adding an extra layer of redundancy of its own. The model achieves this by meeting the following three requirements:

- Get two independent cloud service providers offering equivalent data processing services and two independent cloud service providers offering equivalent data storage services.
- Data replication between both data storage providers is bidirectional and transparent to the user.
- Both data processing services must have access to both data storage services, assumed authorization is granted.

"The Availability Model imposes redundancy on both data processing and cloud storage, hence there is no single point of failure with respect to data access. When a data processing service, or a cloud storage service experiences failure, there is always a backup service present to ensure the availability of the data [20]."

All of the above clearly shows that availability and reliability can be established in multiple and redundant ways, and, therefore are able to contribute to establishing trust in cloud services.

C. Data and Service Migration

Another concern of cloud users is potential lack of long-term service viability and, as a result, the inability to get the data, once placed there, out of the cloud, due to data lock-in with one cloud service provider. In this scenario users would be forced to stay with their cloud service provider, who might request premium prices and thus discourage potential customers to use the cloud service at all. They would only use it, if they really had to, or if they were assured that their data could freely be migrated to other cloud service providers.

Hao, Yen and Thuraisingham consider the problem of service selection and migration in a cloud and developed a framework that simplifies service migration. It also includes a cost model and a genetic decision algorithm to discuss tradeoffs of that matter and find the optimal service migration decisions. In their opinion the important issues surrounding the paper are: "It is necessary to consider the infrastructure support in the cloud to achieve service migration. The computation resources (computer platforms) in the cloud need to be able to support execution of dynamically migrated services. We develop a virtual machine environment and corresponding infrastructure to provide such support. … It is also essential to have a strong decision support to help determine whether to migrate some services and where to place them. The consideration involves the service migration cost, consistency maintenance cost, and the communication cost gains due to migration. We develop a cost model to correctly capture these costs and help determine the tradeoffs in service selection and migration in clouds. Then, we use a genetic algorithm to search the decision space and make service selection and migration decisions based on the cost tradeoffs... [27]."

 ISBN: 978-1-61208-200-4

With their reference deployment model Zhao, Rong, Jaatun and Sandnes go a bit further by stating: "a model that can ensure the capability of migrating data from one cloud to another is imperative… [20]." They demonstrate an abstract model where "the migration of data is guaranteed". The model utilizes a data processing service through which users process their data and that is capable of migrating data from one cloud storage service to another. The model achieves this by meeting the following three requirements:

- There is a Cloud Data Migration Service that can interact with the Cloud Storage Service that keeps users' data for exporting users' data.
- There is a second Cloud Storage Service that allows users to import and export data.
- Two independent cloud providers should provide the two Cloud Storage Services.

Hirofuchi, Ogawa, Nakada, Itoh and Sekiguchi are fulfilling this migration model and believe "the next stage for IaaS cloud technology is cloud federation … users can easily deploy their applications on any IaaS cloud providers in the same manner, and transparently relocate them to other providers on demand [28]." They back up their proposal with an "advanced storage access mechanism that strongly supports live VM migration over WAN. It rapidly relocates VM disks between source and destination sites with the minimum impact on I/O performance. It is implemented as a transparent proxy server for a storage I/O protocol … which can be integrated into SAN services in datacenters. This means that the proposed mechanism is independent of VMM implementations [28]." This counters the risk of data lock-in with a particular provider, while still enabling users to select the most appropriate provider any time with the framework of Hao, Yen and Thuraisingham.

The solutions and proposals in [20][27][28] correspond to the second central point on Ambrust's [9] top ten list of obstacles for growth of cloud computing, namely data lock-in. He thinks standardization of APIs and compatible software enable a surge or hybrid cloud computing. Offering different cloud service selection and migration models, as well as standards, can be used to increase trust in cloud computing.

D. Cryptography

One common way to preserve key requirements, such as confidentiality and integrity in computing, is to encrypt data before, during and even after transport through the Internet for secure storage. As the cloud service provider has access to the data of all its customers, and may offer it, inadvertently or deliberately, to third parties, there is an urgent need for data encryption. One way to conduct this measure is by using combinations of encryption mechanisms. The trust-building and underlying technique used is pre-egression or pre-internet encryption (PIE). This simply means, encrypting data with your own encryption keys before sending it to the cloud. The encryption keys are in possession of the data owner only and are unknown by the cloud service provider or any 3rd party. After the data is encrypted locally it will leave the local premises and transit through the Wide Area Network (WAN). The cloud service provider should not only offer a tunneled and encrypted transit through the network to the storage destination in the cloud. He should also offer encrypted storage of the data. However, since the cloud service provider knows the encryption keys to those tunnels and storage, the only secure method of processing data is the aforementioned PIE.

Pushing the idea of end-to-end encrypted data even further, is the concept of homomorphic encryption. It can be used to conduct mathematic operations on encrypted data without decrypting it [29]. The major and still unsolved downside to this approach is the immense computing power needed to process the encrypted data and limited support for computing operations, which is why this concept is almost unheard of in the public discussion about cloud trust and cloud security.

E. Contractually Fixed Agreements

As stated earlier in the text, trust can be established by establishing control mechanisms. One example of those control mechanisms is Security Service Level Agreements (SSLA) sometimes also referred to as Protection Level Agreements (PLA). They include contractually fixed security restrictions, compliance checks, as well as security information and event management (SIEM). They can be compared to general terms and conditions a company bases its contracts on or to an acceptable use policy (AUP) and are the only legal obligation of the cloud service provider. However, as of today, besides the technical standardization, there are no publicly defined standards yet in the field of information rights management, secure virtual runtime environments and externalization of identities [30][31].

F. Certifications, Standards Compliance and IT Service Quality

Online trust needs a solid and justified foundation to build upon. There are a number of trust-building measures in the field of standards compliance and certifications, three of which we find particularly appealing.

The first trust-building measure that should help choose the right cloud service provider is certifications. Looking at geographical boundaries, there is the Cloud Security Alliance (CSA) in the US and the Federal Agency for Information Security (BSI) in Germany. Both support an initiative called EuroCloud Star Audit that provides a seal of quality for Software-as-a-Service (SaaS), one of the three subdomains of cloud computing. It focuses on topics like data security, data privacy, drafting of contracts and compliance on the one hand, on the other hand, topics such as professional IT management, transparent and comprehensible processes, encryption, backup, archiving, exit-strategy, service level agreements, performance and many more have top priority. By means of a scoring system, cloud service providers are rated with one to five stars, expressing the degree of fulfillment of aforementioned criteria and therefore the trustworthiness. In the near future EuroCloud Star Audit will be expanded to the other two subdomains of cloud computing, namely Platform-as-a-Service (Paas) and Infrastructure-as-a-Service (IaaS), to enable a more complete rating of cloud service providers [32].

 ISBN: 978-1-61208-200-4

The second trust-building measure that should help choose the right cloud service provider is standards compliance. The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) created a series of information security standards, namely the 27000-series. It provides best practice recommendations on information security management, risks and control within the context of an overall Information Security Management System (ISMS). The series is applicable to all types and sizes of organizations and, most importantly, for cloud service providers. Among other topics it covers privacy, confidentiality and IT or technical security issues. The standards series includes ISO/IEC 27001, a standard that specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. It is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. The succeeding standards ISO/IEC 27003, 27004, 27005 and 27006 all refer to the requirements defined in 27001. ISO/IEC 72003 focuses on the critical aspects needed for successful design and implementation of an ISMS. ISO/IEC 27004 provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented ISMS. ISO/IEC 27005 specifies guidelines for information security risk management and ISO/IEC 27006 specifies requirements and guidance for bodies providing audit and certification of an ISMS and is primarily intended to support the accreditation of certification bodies providing ISMS certification [33]. By implementing an ISO/IEC 27001 information security management system, the organization adopts a comprehensive and systematic approach to the security of the process control systems and can therefore be formally audited and certified compliant with the standard.

The third trust-building measure that should help choose the right cloud service provider is IT service quality as defined in the IT Infrastructure Library (ITIL) framework. It is independent of manufacturers, and describes systematic procedures for the strategic development, design, introduction, transition, operation and improvement of IT services. It closely follows ISO/IEC 20000, which provides a formal and universal standard for organizations seeking to have their service management capabilities audited and certified. ITIL version 3, passed in June 2007, consists of five books: Service strategy, service design, service transition, service operation and continual service improvement. Cloud service providers that have aligned their services to the ITIL framework can increase their trustworthiness not only, but mainly because of three ITIL building blocks:

- Information Security Management (ISM)
- Availability Management
- Access Management

ISM ensures most of the information security key concepts: Confidentiality, integrity and availability of an organization's assets, information, data and IT services. Information security is aligned with business security and ISM ensures that information security is effectively managed in all service management processes, activities, etc. The ISM process should be a focal point for all IT security issues and should increase awareness of the need for security within all IT services. A main task of ISM is to produce, maintain and enforce the information security policy.

Availability Management focuses and manages all availability-related issues and is responsible for defining, analyzing, planning, measuring and improving all aspects of the availability of IT services. It ensures that the IT infrastructure and processes, tools, roles etc. are appropriate for the agreed service level targets for availability. This process thus secures the level of availability delivered in all services is matched to, or exceeds the current and future agreed needs of the customers in a cost-effective manner. Availability Management is important because availability and reliability are highly visible to the customers and can directly influence customer satisfaction and the service provider's reputation.

Access Management deals with protecting the confidentiality, integrity and availability of the organization's data and intellectual property. It achieves this by ensuring that only authorized users are able to access or modify the service assets. It provides the right for users to use a service or group of services, while preventing access to non-authorized users. It may also be needed for regulatory compliance reasons. Technologically, Access Management is usually executed by means of directory services [14][34].

All of the three suggested trust-building measures have one thing in common: They prove through examination of a trusted third party that the cloud service provider operates with the necessary care and accuracy required by the presented certifications, standards, frameworks and grants compliance. The willingness of the provider to do so creates transparency for the cloud users and a chance to make a well-informed decision.

G. Transparency

As learned, trust is always a subjective matter, which gives transparency requirements for trust a soft and elastic touch. Transparency has multiple facets though. Trust through transparency can be induced by very simple means such as a web interface design or by more sophisticated means such as a conglomeration of technological factors.

In [11], a framework of four trust-inducing features is proposed by taking existing relevant studies on enhancing online trust by web interface design and using them as dimensions of the framework. The four dimensions are graphic design, structure design, content design and social-cue design. Graphic design refers to the graphical design factors on the web site that normally give consumers a first impression. Structure design defines the overall organization and accessibility of displayed information on the web site. Content design refers to the informational components that can be included on the web site, either textual or graphical. Social-cue design relates to embedding social cues, such as face-to-face

 ISBN: 978-1-61208-200-4

interaction and social presence into web interface via different communication media.

Compared to a trust-inducing web interface design, transparency as add on to technological security mechanisms has much clearer and more precise requirements. Contradicting the often-used principle of security by obscurity, T. Weichert demands security by transparency [31]. He sets up multiple factors on how to reach this goal:

- State of the art measures
- Access restricted to entitled users
- Differentiated access management
- Encryption capabilities
- Anonymization tools
- Adequate separation of data by isolating
- Client-side application security
- Documented data privacy management

His statement is simple to understand: The more of these factors are in place, the higher the transparency and therefore security for cloud service customers will be.

VI. Conclusion and Future Work

Cloud computing services will grow further, regardless of whether a cloud service provider sells services at a low level of abstraction as IaaS, at the medium level as PaaS or at the top level as SaaS. Trust and security go hand in hand - one might even go as far as saying one induces the other.

This paper presented a state of the art overview of the role of trust in cloud computing. Explaining and mapping offline trust to online trust, we showed that the concept of trust does also exist and even plays a vital role in the online world. Trust and security are an integral part of cloud computing and essential for its adoption and growth.

Our main contribution is showing multiple ways to improve online trust and security by leveraging and combining as many existing technology and trust building measures as possible, and by that, minimizing concerns of potential or existing cloud service users. In our opinion, the bottom line of this state of the art overview is, that trust in cloud computing can indeed be improved by means of technology.

A. Limitations

The paper did provide several existing approaches to the issue of insufficient trust and security in cloud computing. However, there are several limitations that have to be acknowledged. The paper did not examine infrastructure issues such as data transfer bottlenecks and performance unpredictability. Computing, storage and networking must all focus on horizontal scalability of virtualized resources rather than on single node performance. Infrastructure in all areas has to be improved, not only in respect to trust and security, but also in respect bandwidth and cost. Furthermore, the paper only highlighted a fractional amount of available security and trust enhancing mechanisms, which we found most important. There are a large number of other efficient mechanisms, standards and an even larger number under investigation in research and development.

B. Future Research and Recommendations

This paper's examples contribute to the ongoing effort of minimizing the challenges regarding trust and security in cloud computing. What still remains is the issue that users have to trust the presented technology, certifications, standards and finally the cloud service provider itself.

Even though trust per definition remains the willingness of a party to be vulnerable to the actions of another party, many unsolved technical issues still exist and many solutions can be improved in order to reduce this inevitable residual risk.

Future research on this topic should include the simplification of cloud security models, for example by standardizing and leveraging protocols, such as the Open Authorization Protocol (OAuth) and the Security Assertion Markup Language (SAML). With the vision of Inter-Cloud-Computing in mind, which introduces an additional management layer above conventional cloud computing systems [35] to reach greater sustainability and availability, large IT companies have to work together more intensely in taskforces, alliances and foundations to push towards this common goal.

Acknowledgment

The authors gratefully acknowledge support from grant 17103X10 from the German federal ministry of education and research.

References

[1] C. Weinhardt, A. Anandasivam, B. Blau, N. Borissov, T. Meinl, W. Michalk, and J. Stößer, "Cloud Computing – A classification, business models, and research directions," *Business & Information Systems Engineering*, 5, pp. 391–399, 2009.

[2] C. Baun, M. Kunze, T. Kurze, and V. Mauch, "Private Cloud-Infrastrukturen und Cloud-Plattformen," *Informatik Spektrum*, vol. 34, no. 3, pp. 242–254, 2011.

[3] Cloud Security Alliance, (2009) "Security guidance for critical areas of focus in Cloud Computing," [Online]. Available: https://cloudsecurityalliance.org/wp-content/themes/csa/guidance-download-box.php [retrieved: April, 2012]

[4] A. Weiss, "Computing in the clouds," *networker*, vol. 11, no. 4, pp. 16–25, 2007.

[5] F. Kamoun, "Virtualizing the datacenter without compromising server performance," *Ubiquity*, vol. 2009, no. August, p. 2, 2009.

[6] A. Greenberg, J. Hamilton, D. A. Maltz, and P. Patel, "The cost of a cloud: research problems in data center networks," *ACM SIGCOMM Comput. Commun.,* vol. 39, no. 1, p. 68, 2009.

[7] B. Hayes, "Cloud Computing," *Comm. ACM*, vol. 51, no. 7, p. 9, 2008.

 ISBN: 978-1-61208-200-4

[8] S. Pearson, "Taking account of privacy when designing cloud computing services," in *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing (CLOUD '09)*, pp. 44–52.

[9] M. Armbrust, I. Stoica, M. Zaharia, A. Fox, R. Griffith, A. D. Joseph, et al., "A view of cloud computing," *Comm. ACM*, vol. 53, no. 4, p. 50, 2010.

[10] J. Bosch, S. Clarke, M. Mowbray, and S. Pearson, "A client-based privacy manager for cloud computing," in *COMSWARE '09 Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middlewaRE*, p. 1, 2009.

[11] Y. D. Wang and H.H. Emurian, "An overview of online trust: Concepts, elements, and implications," *Computers in Human Behavior*, vol. 21, no. 1, pp. 105–125, 2005.

[12] E. H. Erikson, "Childhood and society" (2nd ed.), New York: W.W. Norton, 1963.

[13] M. Deutsch, "Cooperation and trust: Some theoretical notes, " *Nebraska Symposium on Motivation*, 10, pp. 275–318, 1962.

[14] J. B. Rotter, "A new scale for the measurement of interpersonal trust," *J of Personality*, vol. 35, no. 4, pp. 651–665, 1967.

[15] B. Uzzi, "Social structure and competition in interfirm networks: The paradox of embeddedness," *Administrative Science Quarterly*, vol. 42, no. 1, pp. 35–67, 1997.

[16] C. Moorman, R. Deshpande, and G. Zaltman, "Factors affecting trust in market research relationships," *J of Marketing*, vol. 57, no. 1, pp. 81–101, 1993.

[17] Y. Tan and W. Thoen, "Toward a generic model of trust for electronic commerce," *International J of Electronic Commerce*, vol. 5, no. 2 (Winter, 2000/2001), pp. 61-74, 2001.

[18] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," Academy of Management Review, vol. 20, no. 3, pp. 709–734, 1995.

[19] T. H. Noor and Q. Z. Sheng, "Trust as a service: A framework for trust management in cloud environments," pp. 314–321, 2011.

[20] G. Zhao, C. Rong, M. G. Jaatun, and F. E. Sandnes, "Reference deployment models for eliminating user concerns on cloud security," *J of Supercomputing*, 2010.

[21] P. Laue and O. Stiemerling, "Identitäts- und Zugriffsmanagement für Cloud Computing Anwendungen," *Datenschutz und Datensicherheit*, vol. 34, no. 10, pp. 692–697, 2010.

[22] N. Sonehara, I. Echizen, and S. Wohlgemuth, "Isolation in cloud computing and privacy-enhancing technologies," *Business & Information Systems Engineering*, vol. 3, no. 3, pp. 155–162, 2011.

[23] E. Nygren, R. K. Sitaraman, and J. Sun, "The Akamai network; a platform for high-performance internet applications," *SIGOPS Oper. Syst.*, vol. 44, no. 3, p. 2, 2010.

[24] A. Undheim, A. Chilwan, and P. Heegaard, "Differentiated availability in cloud computing SLAs," in *Proceedings of the 2011 IEEE/ACM 12th International Conference on Grid Computing (GRID '11)*, pp. 129–136.

[25] P. Gill, N. Jain, and N. Nagappan, "Understanding network failures in data centers," *SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, pp. 350-361, 2011.

[26] J. M. Hellerstein, S. Chaudhuri, and M. Rosenblum, K. V. Vishwanath, N. Nagappan, "Characterizing cloud computing hardware reliability," in *Proceedings of the 1st ACM symposium on Cloud Computing (SoCC '10)*, p. 193-204, 2010.

[27] W. Hao, I. Yen, and B. Thuraisingham, "Dynamic service and data migration in the clouds," in *Computer Software and Applications Conference, COMPSAC '09. 33rd Annual IEEE International*, pp. 134–139, 2009.

[28] T. Hirofuchi, H. Ogawa, H. Nakada, S. Itoh, and S. Sekiguchi, "A live storage migration mechanism over WAN for relocatable virtual machine services on clouds," in *Proceedings of the 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID '09)*, pp. 460–465.

[29] F. Kerschbaum, "Secure and sustainable benchmarking in clouds," *Business & Information Systems Engineering*, vol. 3, no. 3, pp. 135–143, 2011.

[30] S: Paulus, "Standards für trusted clouds," *Datenschutz und Datensicherheit*, vol. 35, no. 5, pp. 317–321, 2011.

[31] T. Weichert, "Cloud Computing und Datenschutz," *Datenschutz und Datensicherheit*, vol. 34, no. 10, pp. 679–687, 2010.

[32] R. Giebichenstein and A. Weiss, "Zertifizierte Cloud durch das EuroCloud Star Audit SaaS," *Datenschutz und Datensicherheit*, vol. 35, no. 5, pp. 338–342, 2011.

[33] International Organization for Standardization at http://www.iso.org [retrieved: April, 2012]

[34] Materna Information & Communications, (2012), ITIL Version 3 Pocket Guide [Online]. Available: http://www.materna.de/cae/servlet/contentblob/11600/publicationFile/2465/Pocketbrosch%C3%BCre ITIL%C2%AE Version 3.pdf [retrieved: April, 2012]

[35] T. Aoyama and H. Sakai, "Inter-cloud computing," *Business & Information Systems Engineering*, vol. 3, no. 3, pp. 173–177, 2011.

 ISBN: 978-1-61208-200-4