Turning Dark into White Clouds – A Framework on Trust Building in Cloud Providers via Websites

Completed Research Paper

Ayten Öksüz
University of Muenster, ERCIS
ayten.oeksuez@uni-muenster.de

Abstract

Due to concerns about data security and privacy and the lack of trust, many individuals and organizations are reluctant to use cloud services. Thus, gaining users' trust in cloud computing is considered as a challenge faced by cloud providers. Previous studies in the field of trust and cloud computing mainly focus on technical aspects such as improving security. While this is important, trust is also shaped by perceptions which in turn are influenced by communication. However, this understanding of trust has been neglected in cloud computing literature so far. This paper conceptualizes the relationships between trust in cloud providers, security, risks, perceptions, and communication in a framework. Based on this understanding, previous literature in the field of trust and cloud computing is analyzed. As a result, future research should explore how cloud providers can improve the communication of implemented security and privacy measures in order to enhance trust.

Keywords

Cloud computing, trust, websites, online risk perceptions, security, communication.

Introduction

The current hype of Cloud Computing (CC) is shaped by opportunities and risks. The use of CC entails various positive aspects such as remote access of data, scalability and cost-reduction (Lee 2010). However, many individuals and organizations are skeptical towards the internet and internet-based technologies like CC (Fortinet 2013). As a consequence, a lack of trust and reluctance in adoption restricts CC to expand its full potential (Garrison et al. 2012).

Gaining customers' trust is a twofold challenge for CC providers. Previous studies in the field of trust and CC have shown that the focus mainly lies on improving security (Yang and Tate 2012). More precisely, articles mainly analyze, for example, how the security of CC's technical infrastructure can be improved, or access can be controlled (Yang and Tate 2012). As there are actual risks due to the web-based character of CC, improving security measures is important. However, besides these technical aspects, literature neglects the fact that trust is shaped by perceptions (Mayer, Davis, Schoorman 1995). This highlights the fact that a distinction between actual trustworthiness and the perceived trustworthiness of another party has to be made (Chellappa and Pavlou 2002).

One prominent way of shaping perceptions about the trustworthiness of another party is communication via websites (Wang and Emurian 2005). While communication in general is an important factor in assessing the trustworthiness of another party, in the digital age, information is often collected online. For online providers, such as CC providers, a primary way of communicating is via websites (Wang and Emurian 2005). While there has been a structured evaluation of trust building via websites (Karimov and Brengman 2011), the specific requirements for trust building in CC have not been analyzed. In the context of CC, its risks and need for trust, it is important to understand how actual circumstances and perceptions with regard to security and privacy measures via websites relate to each other. This study addresses this research gap by, first, developing a framework of these relationships, and, second, reviewing the literature

in the field along the framework dimensions. The developed framework focuses on trust between an individual user and an organization (organizational trust).It may also be applicable to trust relationships between two organizations (inter-organizational trust). The latter step, a comparison with existing theory, gives insight in how far the relationships between trust, CC, and websites have been analyzed before which is a basis for implications for future research.

The paper is structured as follows: First, we outline the theory of trust and its elements. As a result, we develop a framework on trust building in cloud providers via websites. Second, we analyzed current literature on trust in the context of CC according to the developed framework. Finally, we discuss the results and conclude with some implications and a future research agenda.

Cloud Computing

According to the definition of the National Institute of Standards and Technology (NIST), CC is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with a minimal effort or service provider interaction as a pool of computing resources" (Mell and Grance 2011). There are three types of CC service models: Software as a service (SaaS), which provides access to software remotely as a web-based service (Mell and Grance 2011), Platform as a service (PaaS), which provides a computing platform to allow users to build applications and services over the internet, and infrastructure as a service (IaaS), where computing resources such as storage is provided through the internet (Mell and Grance 2011). Two main deployment models can be distinguished: A private cloud is exclusively used by a single institution whereas a public cloud is used by the general public (Mell and Grance 2011). While in the case of private clouds, the physical location of the cloud infrastructure can be either off premise or on premise, in the case of public clouds, the cloud infrastructure only can exist on the premises of the cloud provider (Mell and Grance 2011). Trust in a CC provider depends to a great extent on the selected deployment model (Zissis and Lekkas 2012). In the case of public clouds, governance of data or applications is outsourced and control is delegated to the CC provider owning the infrastructure (Zissis and Lekkas 2012). Users then have to trust that adequate security and privacy measures are implemented by the provider in order to guarantee data security and privacy (Zissis and Lekkas 2012). Since users are not able to fully control whether and which security and privacy measures are in place, they are exposed to high security and privacy risks. In the case of private clouds, the infrastructure is operated and managed on premise by the data or process owner (Zissis and Lekkas 2012). Such a situation does not introduce additional risks as control remains with the data or process owner (Zissis and Lekkas 2012). As public clouds pose higher risk on users than private clouds, in the following, the paper focuses on public clouds.

Characteristics and Elements of Trust

Definition of Trust and Parties of the Trust Relationship

Mayer et al. (1995) define trust as the "willingness of a party [trustor] to be vulnerable to the actions of another party [trustee] based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (p.712). A trustor as well as a trustee can be an individual, a group of persons or an organization (Mayer et al. 1995). In this sense, there is a distinction between interpersonal, organizational and inter-organizational trust. Interpersonal trust means the trust relationship between two individuals or groups (Rotter 1967). Organizational trust focuses on an individual's trust in an organization (Mayer et al. 1995). Inter-organizational trust is relevant in business-to-business relationships and is defined as the extent to which the members of an organization have a collectively-held trust orientation toward the partner organization (Zaheer et al. 1998). In the context of CC, the trustor is typically either an individual or an organization who consider whether to use a cloud service or not. The trustee is mostly the provider of cloud services, also called CC provider. In the following, the paper focuses on organizational trust.

Factors of Perceived Trustworthiness

The trustor evaluates the trustworthiness of the trustee based on certain characteristics and actions of the trustee (Mayer et al. 1995). There are three trustee characteristics which explain the trustee's trustworthiness: ability, benevolence, and integrity (Mayer et al. 1995). Ability is the group of skills, knowledge, and expertise that enable the trustee to perform a specific task (Mayer et al. 1995). Benevolence refers to the perception of the trustee's positive orientation towards the trustor. It is defined as "the extent to which a trustee is believed to want to do good to the trustor", apart from egoistic profit motives (Mayer et al. 1995). Integrity means that the trustee observes a set of principles that the trustor appreciates (Mayer et al. 1995). Research on trust within the IS discipline mostly deal with trust problems in the context of e-commerce, such as the development of trust in an internet merchant (Chellappa and Pavlou 2002; Gefen 2002; Kim and Benbasat 2003). Kim and Benbasat (2003), for example, show specific issues that influence consumers' trust in an internet merchant. Based on their work, we derive relevant trust related characteristics in the context of CC (see table 1).

	Relevant trust-related characteristics in the context of e-commerce	Relevant trust-related characteristics in the context of CC
Ability	Knowledge, skills, and resources important for the internet merchant to provide the following: • Products of good quality • On-time delivery • After sales support • Secure handling of sales transactions • Protection of personal data • Advice and information	Knowledge, skills and resources important for the CC provider to provide the following: • A service of good quality • High availability • (Technical) Support • Secure data transfer (e.g. with the use of SSL) • Protection of personal data and data stored in the cloud • Advice and Information
Integrity	• Merchant does not collect unnecessarily personal information and does not hide the purpose of information gathering • Merchant establish acceptable policies, which protect users' rights	• Cloud provider does not collect unnecessarily personal information and does not hide the purpose of information gathering • Cloud provider establish acceptable policies, which protect users' rights
Benevolence	• Merchant acts in the interest of users • Merchant does not focus on profit maximization	• Cloud provider acts in the interest of users • Cloud provider does not focus on profit maximization or cost reduction by, for example, reducing expenditures on data security and privacy

Table 1. Trust Related Characteristics in the Context of CC

Trust as an Influencing Factor of Intention to Use Technology

In the IS discipline trust is seen as an important factor influencing the acceptance and adoption of (new) technologies (Gefen et al. 2003). For example, the technology acceptance model (TAM), has been

expanded by the factor trust (Gefen et al. 2003). Accordingly, beyond perceived ease of use (PEOU) and perceived usefulness (PU), the intention to use a new IT depends on trust (Gefen et al. 2003). In the context of CC, this means that trust influences whether an individual intent for example to store his/her (sensitive) data in the cloud (or on the servers of the cloud provider). In the case of companies which have the possibility to store customer data in the cloud, this is an even more difficult matter, since companies deal with very sensitive customer data.

Perceived Risk

The definition of trust implies that any trust relationship involves vulnerability. Making oneself vulnerable means to take a risk (Mayer et al. 1995). In this sense, trust is a key influencing factor of action in a situation in which perceived risk of negative outcome exists (Luhmann 1979). If the level of trust surpasses the threshold of perceived risk, then the trustor will take a risk (Mayer et al. 1995). If the level of perceived risk is greater than the level of trust, the trustor will not take a risk (Mayer et al. 1995). Thus, in the context of CC, the trustor's perceived risk moderates the effect of trust on the intention to use CC services. Due to the complexity and the anonymity associated with online interactions users often are uncertain about the risks at present and their possible consequences when transacting online (Wang and Emurian 2005). This also applies for CC which is composed of service models provided through the internet. The root of the problem is that users lose the physical control of their (confidential) data when they store their data or place their applications on servers in a CC environment. In the case of e-commerce, three types of risks have been identified (Pavlou 2003): product risk, financial risk, and information risk (security and privacy). In the context of CC, there are no product risks, but risk relating to the service quality such as an insufficient availability of the service or system failures (Zissis and Lekkas 2012). Financial risks means, that users could suffer a financial loss when purchasing a product or using a service via the Internet for example as a result of credit card fraud (Bhatnagar et al. 2000). Information risk is associated with data security and data privacy (Pavlou 2003). There is, for example, the risk that third parties or hackers get access to sensitive data of users and do harm such as identity theft (Zissis and Lekkas 2012). Besides these mentioned three types of risks, the use of CC also entails legal risk (Zissis and Lekkas 2012). This is due to the fact that the cloud providers' servers, where users' or companies' data are stored, could be physically located anywhere (e.g. Europe, Asia, USA) (Zissis and Lekkas 2012). Moreover, the data could be stored in multiple locations, so that users often neither can control nor do know the exact location of their data (Zissis and Lekkas 2012). When data are transferred across jurisdictional borders, legal protection could be reduced (Pearson and Benameur 2010).

Perceptions vs. Actuality

As trust is a perception, analyzing users' trust in a cloud provider requires a distinction between actual and perceived trustworthiness of a provider (Chellappa and Pavlou 2002). A provider's actual trustworthiness refers to a provider's actual ability and willingness to secure users' data and to ensure data privacy (Chellappa and Pavlou 2002). Thus, the actual trustworthiness depends on the (technical) measures implemented by a provider to protect users' (personal) data and privacy (Chellappa and Pavlou 2002). Using the latest security and privacy measures such as encryption or access control will lead to a higher actual data security and privacy protection. Furthermore, the implemented security and privacy measures have to work properly (Chellappa and Pavlou 2002). A high actual data security and privacy protection means that a provider is actually able and willing to protect users' (personal) data and thus, is actually trustworthy. However, the perceived trustworthiness represents a personal anticipation and intuitive perception rather than an objective measurement (Chellappa and Pavlou 2002). The perceived trustworthiness is the extent to which a potential user believes that a provider is able and willing to ensure data security and privacy of the user (Chellappa and Pavlou 2002). This in turn depends on a user's perceived data security and privacy protection. Perceived data security and privacy protection is the subjective probability with which users believe that their (personal) data will be protected against third party access or hacker attacks during data transfer and when stored in the cloud (Chellappa and Pavlou 2002). Users will perceive a provider as being trustworthy when they believe that the provider will comply with security requirements by implementing security measures such as encryption and access control (Kim et al. 2008). This also entails the belief that a provider will respect users' privacy and will not collect unnecessarily personal data. In this sense, consumer's perceived security and privacy protection has a positive effect on user's trust (Kim et al. 2008). Furthermore, it is stated that perceived data security and

privacy protection negatively affects user's perceived risk (Kim et al. 2008; Pavlou et al. 2007). The perceived trustworthiness of a provider does not necessarily reflect the actual trustworthiness of a provider (Chellappa and Pavlou 2002). A provider might be perceived as not trustworthy although the provider is actually trustworthy and vice versa. It is, for example, possible that a provider is actually able and willing to protect user's data by using the latest security and privacy measures. However, potential users might not believe in the ability and willingness of the provider. Thus, for users' trust, actual trustworthiness is important, but the perceived trustworthiness of a provider is what really matters. The question arises, what determines the perception of a provider's ability and willingness to protect users' data and thus a provider's trustworthiness? Communication is instrumental in the formation of these perceptions (Rogers, 2003).

Trust through Communication via Websites

Communication is one of the main elements that influence the development of perceptions (Rogers 2003). In this sense, communication determines whether a cloud provider is perceived as being trustworthy or not. For example, a provider might use the latest security and privacy measures and thus is able and willing to protect users' (personal) data. However, it could be that users do not perceive a high security and privacy protection when provider's communication of the implemented security and privacy measures is insufficient. In the first instance, using the latest security and privacy measures is the basis for trust by enhancing more or less the actual data security and privacy. However, focusing solely on the implementation of new security and privacy measures for a higher actual security and privacy protection is insufficient since it does not per se lead to more user trust.

Online providers (organizations, merchants, shops etc.) use primarily their websites to attract potential users and to communicate with them (Wang and Emurian 2005). Thus, online providers have to apply trust-inducing features to their website in order to enhance users' trust (Wang and Emurian 2005). This also applies for CC providers, since they provide their services mainly through the internet. Karimov et al. classify trust-inducing website features according to three broad dimensions, namely visual design, content design, and social cue design (Karimov and Brengman 2011). Visual design is defined as "the attention-grabbing, aesthetic, visual quality of individual Web pages" (Demangeot and Broderick 2010). Visual design deal with graphical design features such as the use of product images and colors and with the structure design such as navigation aids and layout of information (Wang and Emurian 2005). Content design refers to "the informational components that can be included on the web site, either textual or graphical" (Wang and Emurian 2005). Social cue design deals with embedding social cues into the website to give a feeling of social presence or face-to-face interaction (Pavlou et al. 2007). Content and social cue design dimensions are especially suitable for helping a provider to convey his or her ability and willingness to protect users' data security and privacy. With regard to content design dimension, it is important to communicate implemented security and privacy measure in such a way that users perceive a provider as being trustworthy. Referring to social cue design dimension, a provider has to reduce the perceived social distance between users and the provider.

Communicating Implemented Security and Privacy Measures

Cloud providers have to verify that they are able and willing to protect users' (personal) data and privacy. Research in the context of online trust and e-commerce state, that online merchants have various options available for this purpose. On the one hand, they can provide security and privacy policies that give information about implemented privacy and security measures (Belanger et al. 2002). In security and privacy policies a provider makes statements, for example, about data collected, data sharing policies, and security features such as encryption (Belanger et al. 2002). The technical aspects of data security and privacy measures are often too complicated for users to fully understand (Anton et al. 2007). However, users must be able to understand the security and privacy policies in order to assess provider's trustworthiness (Anton et al. 2007). How users perceive security and privacy protection depends on how clearly they understand the level of security and privacy measures implemented by the provider (Friedman et al. 2000). One way to communicate complex (technical) issues in clear and easily understandable terms is using visualizations (Glenberg and Langston 1992). Visualizations are illustrations of textual descriptions (e.g. graphs), depicting specific elements of a text (Glenberg and Langston 1992). On the other hand, online merchants can use third party seals or certificates. Third-party

seals assure users that a provider is trustworthy (Wang and Emurian 2005). Third-party seals are particularly relevant for online providers which are unfamiliar to users (Pavlou and Gefen 2004) and can verify that a provider protect privacy and provide security. Several studies have shown that these assurance symbols are effective in establishing trust trough trusted third parties, such as TRUSTe (Wang and Emurian 2005).

Reducing Perceived Social Distance

Data privacy and security concerns associated with online interactions often arise due to the physical separation or perceived social distance between users and sellers (Choi et al. 2001). It is known that social presence shortens the perceived social distance between users and sellers by making users believe that the online interaction is similar to face-to-face interactions (Kumar and Benbasat 2002). Social presence creates a perceptual illusion in which users perceive a distant entity as being close (Choi et al. 2001). Social presence is built on cues, such as pictures of employees, recommendation agents or virtual agents, and IT-enabled human-like interaction (Pavlou et al. 2007). There are various investigations in the context of e-commerce showing that social presence has a positive influence on trust and mitigates perceived data security and privacy risk (Cyr et al. 2009; Pavlou et al. 2007). Thus, in the context of CC, social presence might also mitigate data privacy and security concerns or might positively influence perceived data security and privacy protection by reducing the social distance between users and CC providers.

Developing a Framework on Trust Building in the context of Cloud Computing

All the above mentioned aspects of trust and findings from the field of trust in e-commerce and online trust conclude to the following framework (figure 1). Regarding the visual design of the framework, we were inspired by (Walter et al. 2013):

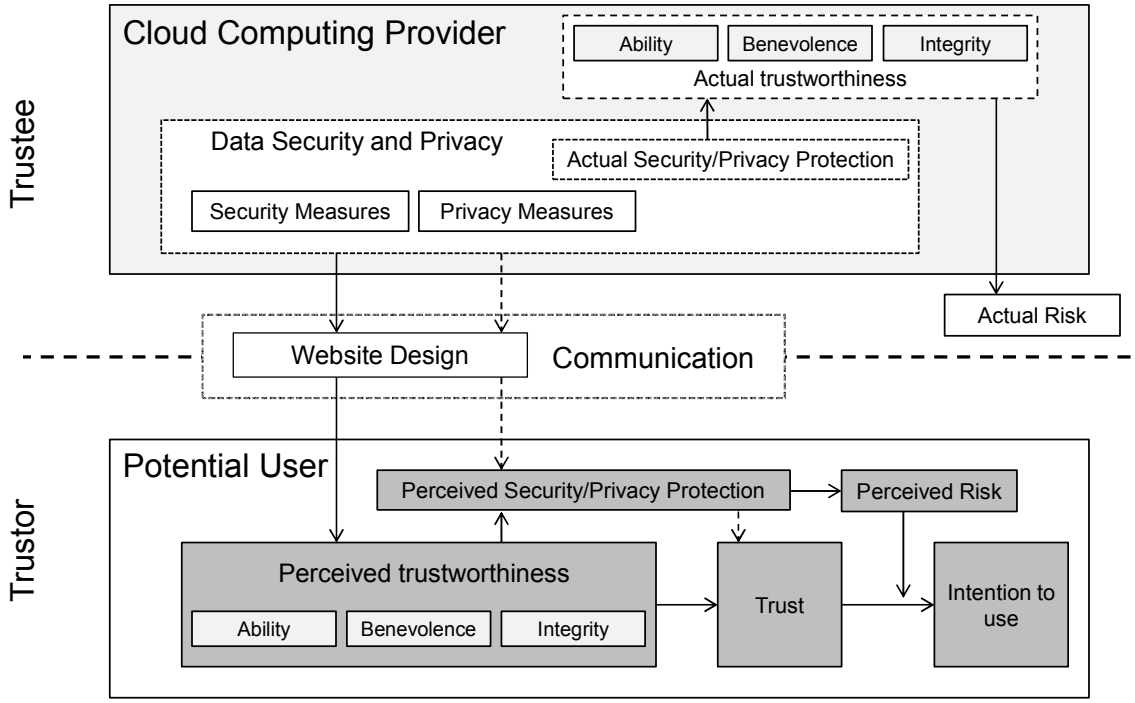

Figure 1: A Framework on Trust Building in Cloud Providers via Websites

Research Methodology

To analyze research on trust in the context of CC and to address the research gap, a structured literature review was conducted as suggested by Webster and Watson (2002). First step was a search process with a keyword search in the scholarly database Web of Science. The search string was as follows: TOPIC: ["cloud computing" OR "cloud" OR "clouds" OR "Infrastructure as a Service" OR "IaaS" OR "Software as a Service" OR "SaaS" OR "Platform as a Service" OR "PaaS"] AND TOPIC: [“trust” OR “trustworthiness” OR “Confidence”]. The search was carried out on February 10th 2014 and the number of hits was 121. Most of the articles were not relevant and were filtered out, since they did not deal with trust-building in the context of CC. Second, by reading the title, keywords, and abstract, relevant articles were identified. Thus, after an initial evaluation and selection, 37 papers remained. However, more than half of the 37 papers turned out to be not relevant, since they only focus on technological issues. They used the term “trust” synonymously with “security” referring to technological security precautions to enhance the security of the cloud infrastructure. Finally, nine relevant articles fit the criteria and were analyzed according to the built framework in the related work section. We examined, whether the articles dealt with or considered the following elements of our framework:

Element of the framework	Abbreviation
Actual trustworthiness	AT
Data Security and Privacy Measures	DSP
Actual Security and Privacy	ASP
Actual Risk	AR
Website Design: Communicating Implemented Security and Privacy Measures	CSP
Website Design: Reducing Perceived Social Distance	PSD
Perceived Security and Privacy	PSP
Perceived Risk	PR
Perceived Trustworthiness	PT
Trust	T
Intention to Use	IU

Table 2. Abbreviations

Results

An overview of the results is presented in table 3. Five articles consider communication, transparency or the willingness to share information as very important for trust-building in CC provider (Chou and Chiang 2013; Garrison et al. 2012; Khan and Malluhi 2010; Ouedraogo and Mouratidis 2013; Pearson 2011). Most of them state that communicating implemented security and privacy measures are important in order to enable users to assess a provider’s trustworthiness. Only one empirical article considers communication as an independent variable in the study and shows that verifying the ability and willingness to protect users’ data and privacy has an influence on user’s trust in the cloud provider (Chou and Chiang 2013). Nevertheless, very few explore *how* cloud providers should communicate their implemented security and privacy measures in order to enhance users’ perceived security and privacy protection and to be perceived as being trustworthy. Only two theoretical articles suggest that cloud providers should use certificates in order to enhance trust (Khan and Malluhi 2010; Ouedraogo and Mouratidis 2013). One of the article state that a certification from an independent third party would be more credible than verifying security protection only with statements (Ouedraogo and Mouratidis 2013). Another one posits that cloud providers should give information about the physical location of their servers in order to establish trust

(Khan and Malluhi 2010). One article proposes an approach as a way to mitigate the perceived uncertainties associated with CC. The approach helps to determine the adequacy of a provider's implemented set of security measures by assessing its completeness in addressing most of the risks associated with the CC (Ouedraogo and Mouratidis 2013). The same paper addresses the fact that users do not always have the technical knowledge to assess the adequacy of a cloud provider's security and privacy. None of the articles deal with the use of social presence in order to establish trust in the context of CC.

Author (Year)	Topic	AT	DSP	ASP	AR	CSP	PSD	PSP	PR	PT	T	IU
Chou et al. (2013)	The Effect of trust on SaaS satisfaction	X				X		X	X	X	X	
Oudraogo (2013)	An Approach for Selecting a Cloud Service Provider					X		X	X	X	X	
Garrison et al. (2012)	Factors influencing cloud Deployment Success				X	X		X		X	X	X
Pearson (2011)	The Importance of Accountability for trust-building in CC	X		X		X		X	X	X		
Wu (2011b)	Factors affecting the adoption of SaaS							X			X	X
Wu (2011a)	Factors affecting the adoption of SaaS							X		X	X	X
Wu et al. (2011)	Factors affecting an organization's SaaS adoption								X	X	X	X
Heart (2010)	Effect of trust and perceived risk on the intention to adopt SaaS							X	X	X	X	X
Khan et al. (2010)	How can cloud providers earn user's trust	X	X	X		X		X		X	X	

Table 3. Overview of the Results

Discussion and Conclusion

The results of the literature review shows that only half of the articles emphasize the importance of communicating implemented security and privacy measures for trust building in the context of CC. Nevertheless, CC poses increased security and privacy challenges for users compared to traditional systems such as in e-commerce. This fact has three main implications.

First, more than in the context of e-commerce, users must be able to understand the security and privacy policies in order to assess a provider's trustworthiness. However, users often do not fully understand the technical aspects of data security and privacy measures. Furthermore, security and privacy policies

sometimes include too much information so that users perceive information overload. Thus, it is not sufficient just to communicate implemented security and privacy measures, but providers have to consider *how* they communicate these measures. The results of the literature review shows that there are very few articles addressing this fact. Consequently, future research has to analyze, how certain information regarding data security and privacy issues should be communicated and how security and privacy policies should be designed in order to enhance trust. This also entails the question, how the technical aspects can be explained in order to be understandable. Using visualizations such as graphs is one way to reduce information overload or to enable a deeper understanding of complex (technical) issues (Glenberg and Langston 1992). Experimental studies should be conducted in order to test the effect of different ways to communicate security and privacy issues on trust.

Second, in the context of CC, users might have different information needs regarding data security and privacy compared to the e-commerce context (see table 1). Thus, future research should analyze which specific information regarding security and privacy protection should be communicated in order to establish trust. One of the paper, for example, state that providers should give information about the physical location of their server where data are stored. In future experiments it could be empirically tested, whether users' trust in a cloud provider increases when the location of servers is communicated.

Third, users' perceived risk regarding data security and privacy might be higher than in the e-commerce context. Thus, it is very important for cloud providers to know how they can mitigate users' perceived risk. One way to do so is making use of social presence. Future research should analyze, whether the positive influence of social presence on trust, as tested in e-commerce, also holds true in the context of CC. More precisely, it should be analyzed, whether pictures of employees, and recommendation or virtual agents should be embedded in a provider's website in order to enhance trust. The design of such an agent might also play a role and has to be chosen appropriately. Should the agent, for example, be a male or a female, old or young, resemble an IT manager or a businessman. In addition, a website analysis of current CC provider should be conducted in order to get an idea if and to what extent social presence is used in practice. Another way to reduce perceived risk is to communicate specific information about risks (Lipkus and Hollands 1999). In some cases, the perceived risk might be higher than the actual risk. In those cases, using visualizations can mitigate users' perceived risk by pointing out that the risk at present is not as high as previously perceived. Therefore, future research should explore how visual communication of risks can be used in the context of CC.

In summary, besides seeking for new technical measures to improve the protection of sensitive data in the cloud, efforts should be put in research on how to better communicate implemented security measures in order to enhance trust in cloud providers.

Acknowledgements

The author would like to thank the Track Chair, Mini-Track Chair, and reviewers for their excellent comments and suggestions that have improved the quality of this paper.

The presented work was supported by the German Research Foundation (DFG): research project "Trust and Communication in a Digitized World", promotion sign 1712/1.

REFERENCES

Anton, A.I., Bertino, E., Li, N., and Yu, T. 2007. "A Roadmap for Comprehensive Online Privacy Policy Management," *Commun. ACM* (50:7), pp. 109-116.

Belanger, F., Hiller, J.S., and Smith, W.J. 2002. "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes," *The Journal of Strategic Information Systems* (11:3–4), pp. 245-270.

Bhatnagar, A., Misra, S., and Rao, H.R. 2000. "On Risk, Convenience, and Internet Shopping Behavior," *Commun. ACM* (43:11), pp. 98-105.

Chellappa, R.K., and Pavlou, P.A. 2002. "Perceived Information Security, Financial Liability and Consumer Trust in Electronic Commerce Transactions," *Logistic Information Management* (15:5/6), pp. 358-368.

Choi, Y.K., Miracle, G.E., and Biocca, F. 2001. "The Effects of Anthropomorphic Agents on Advertising Effectiveness and the Mediating Role of Presence," *Journal of Interactive Advertising* (2:1), pp. 19-32.
Chou, S.-W., and Chiang, C.-H. 2013. "Understanding the Formation of Software-as-a-Service (Saas) Satisfaction from the Perspective of Service Quality," *Decision Support Systems* (56:0), pp. 148-155.
Cyr, D., Head, M., Larios, H., and Pan, B. 2009. "Exploring Human Images in Website Design: A Multi-Method Approach," *MIS Q.* (33:3), pp. 539-566.
Demangeot, C., and Broderick, A.J. 2010. "Consumer Perceptions of Online Shopping Environments: A Gestalt Approach," *Psychology and Marketing* (27:2), pp. 117-140.
Fortinet. last access on 18.11.2013. "Internet Security Census 2013 - a Fortinet Global Survey," *http://www.fortinet.com/sites/default/files/surveyreports/Fortinet-Internet-Security-Census-2013.pdf* .
Friedman, B., Peter H. Khan, J., and Howe, D.C. 2000. "Trust Online," *Commun. ACM* (43:12), pp. 34-40.
Garrison, G., Kim, S., and Wakefield, R.L. 2012. "Success Factors for Deploying Cloud Computing," *Commun. ACM* (55:9), pp. 62-68.
Gefen, D. 2002. "Reflections on the Dimensions of Trust and Trustworthiness among Online Consumers," *SIGMIS Database* (33:3), pp. 38-53.
Gefen, D., Karahanna, E., and Straub, D.W. 2003. "Trust and Tam in Online Shopping: An Integrated Model," *MIS Quarterly* (27:1), pp. 51-90.
Glenberg, A.M., and Langston, W.E. 1992. "Comprehension of Illustrated Text: Pictures Help to Build Mental Models," *Journal of Memory and Language* (31:2), pp. 129-151.
Heart, T. 2010. "Who Is out There?: Exploring the Effects of Trust and Perceived Risk on Saas Adoption Intentions," *SIGMIS Database* (41:3), pp. 49-68.
Karimov, F.P., and Brengman, M. 2011. "Adoption of Social Media by Online Retailers: Assessment of Current Practices and Future Directions," *International journal of e-entrepreneurship and innovation* (2:1), pp. 26-45.
Khan, K.M., and Malluhi, Q. 2010. "Establishing Trust in Cloud Computing," *It Professional* (12:5), Sep-Oct, pp. 20-26.
Kim, D., and Benbasat, I. 2003. "Trust-Related Arguments in Internet Stores: A Framework for Evaluation," *Journal of Electronic Commerce Research* (4:2), pp. 49-64.
Kim, D.J., Ferrin, D.L., and Rao, H.R. 2008. "A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents," *Decision Support Systems* (44:2), pp. 544-564.
Kumar, N., and Benbasat, I. 2002. "Para-Social Presence and Communication Capabilities of a Web Site: A Theoretical Perspective," *E-service Journal* (1:3), pp. 5-24.
Lee, C.A. 2010. "A Perspective on Scientific Cloud Computing," in *Proceedings of the 19th ACM International Symposium on High Performance Distributed Computing*, Chicago, IL: ACM, pp. 451-459.
Lipkus, I.M., and Hollands, J.G. 1999. "The Visual Communication of Risk," *JNCI Monographs* (1999:25), January 1, 1999, pp. 149-163.
Luhmann, N. 1979. *Trust and Power*. Chichester, UK: Wiley.
Mayer, R.C., Davis, J.H., and Schoorman, F.D. 1995. "An Integrative Model of Organizational Trust," *The Academy of Management Review* (20:3), pp. 709-734.
Mell, P., and Grance, T. 2011. "The Nist Definition of Cloud Computing (Draft) Recommendations of the National Institute of Standards and Technology," in: *The National Institute of Standards and Technology (NIST)*. Gaithersburg.
Ouedraogo, M., and Mouratidis, H. 2013. "Selecting a Cloud Service Provider in the Age of Cybercrime," *Computers & Security* (38:0), pp. 3-13.
Pavlou, P.A. 2003. "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model," *International Journal of Electronic Commerce* (7:3), Spr, pp. 101-134.
Pavlou, P.A., and Gefen, D. 2004. "Building Effective Online Marketplaces with Institution-Based Trust," *Info. Sys. Research* (15:1), pp. 37-59.
Pavlou, P.A., Liang, H., and Xue, Y. 2007. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective," *MIS Quarterly* (31:1), pp. 105-136.
Pearson, S. 2011. "Toward Accountability in the Cloud," *Internet Computing, IEEE* (15:4), pp. 64-69.
Pearson, S., and Benameur, A. 2010. "Privacy, Security and Trust Issues Arising from Cloud Computing," *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on*, pp. 693-702.
Rogers, E.M. 2003. *Diffusion of Innovations*. New York: Free Press.

Rotter, J.B. 1967. "A New Scale for the Measurement of Interpersonal Trust1," *Journal of Personality* (35:4), pp. 651-665.

Walter, N., Ortbach, K., Niehaves, B., and Becker, J. 2013. "Trust Needs Touch: Understanding the Building of Trust through Social Presence," *in Proceedings of the 19th Americas Conference on Information Systems*, Chicago, IL.

Wang, Y.D., and Emurian, H.H. 2005. "An Overview of Online Trust: Concepts, Elements, and Implications," *Computers in Human Behavior* (21:1), pp. 105-125.

Wu, W.-W. 2011a. "Developing an Explorative Model for Saas Adoption," *Expert Systems with Applications* (38:12), pp. 15057-15064.

Wu, W.-W. 2011b. "Mining Significant Factors Affecting the Adoption of Saas Using the Rough Set Approach," *Journal of Systems and Software* (84:3), pp. 435-441.

Wu, W.-W., Lan, L.W., and Lee, Y.-T. 2011. "Exploring Decisive Factors Affecting an Organization's Saas Adoption: A Case Study," *International Journal of Information Management* (31:6), pp. 556-563.

Yang, H., and Tate, M. 2012. "A Descriptive Literature Review and Classification of Cloud Computing Research," *Communications of the Association for Information Systems* (31:2), pp. 35-60.

Zaheer, A., McEvily, B., and Perrone, V. 1998. "Does Trust Matter? Exploring the Effectsof Interorganizational and Interpersonaltrust on Performance," *Organization Science* (9:2), pp. 141-159.

Zissis, D., and Lekkas, D. 2012. "Addressing Cloud Computing Security Issues," *Future Generation Computer Systems-the International Journal of Grid Computing and Escience* (28:3), pp. 583-592.