Unboxing Trust in Cloud Computing. A Survey Study

Nils Backhaus and Stefan Brandenburg [a]

[a] *Chair of Cognitive Psychology and Cognitive Ergonomics*
Technische Universität Berlin, Germany
Sekr. MAR 3-2, Marchstr. 23, D-10587 Berlin

ABSTRACT

Cloud computing is a vital change in the way we process and store data. Having data stored inside the cloud, it is not physically present on the user's hard drive. Therefore he or she is no longer involved in the collection, processes, storage and disclosure of this data (Cavoukian, 2008). This makes the user more vulnerable, especially in the case of sensitive data (Onwubiko, 2010). The present survey tries to unravel the facets of trust in cloud services and the usage of a cloud storage service, Dropbox. Factors from the Technology Acceptance Model (TAM), privacy and security, reputation, and personal innovativeness were included in a research model and assessed with a questionnaire. The results of the questionnaire analysis show the importance of privacy and security as well as reputation in building trust. The TAM seems to be associated with trust and moderating the influence of trust on the usage of Dropbox. Finally, theoretical assumptions and practical implications of the findings are discussed highlighting the importance of trust in cloud computing and all fields of information system research.

Keywords: Cloud Computing, Trust, Online Trust, Privacy, Security, Dropbox, Technology Acceptance Model

INTRODUCTION

The *cloud* is a buzzword in information and communication technology (ICT). It describes the technological transition how we store and process data moving from offline to online computing. The term *cloud computing* means to entrust data to systems that are managed by external parties on remote servers. Using cloud computing influences several ICT processes and the users involved in those processes. On the one hand processing data becomes more flexible and cost-effective because of ubiquitous network access, on-demand self-service models, and elastic resources. On the other hand new challenges as to privacy, security, and trust arise, since the user is not involved in the collection, processing, storage, and disclosure of his data anymore (Cavoukian, 2008).

The following examination of trust in cloud computing scrutinizes several aspects of *the cloud* focusing on features that are related to trust. Therefore we will look upon trust, trust antecedents, and trust outcomes in relation to cloud computing. Since there is no empirical approach directly dealing with trust in cloud computing, neighboring fields like online trust (e-commerce), acceptance of information systems, and trust in technology are reviewed to build a model for an empirical investigation of the topic.

https://openaccess.cms-conferences.org/#/publications/book/978-1-4951-2096-1

Cloud Computing

Cloud Computing is a new way to store and process data remotely by virtualization of scalable computing resources (Armbrust et al., 2009). By definition, Cloud Computing is characterized by the following key points (Mell & Grance, 2011):

- On demand self-service: consumers can automatically modify resources;
- Broad network access: virtualized resources can be accessed over the network by various devices from any place, given network access;
- Resource pooling: Providers offer pooled resources in a multi-tenant model and assign and reassign resources as much as the consumer needs. The consumer has no control or knowledge about the exact location of the provided, abstracted resources (e.g. state, city, data center, and server);
- Rapid elasticity: The service can be scaled horizontally and vertically rapidly and elastically, and in some cases even automatically according to the consumer's demands;
- Measured service: This involves an automatic control and optimization of resources. The use of the resources is monitored and controlled, providing transparency to provider and consumer.

This broad definition is suitable for a lot of our daily services. Consider, for example, Dropbox, Facebook or Microsoft Office 365, all of them use cloud resources. Even programmers and developers utilize cloud-based resources like Google AppEngine or Microsoft Azure. In most cases, these services use servers provided by data giants, e.g. Amazon, Microsoft, Google, or IBM (Ryan, 2013).

In other words, the cloud community follows a structural definition and describes basically three service levels as well as three deployment models (Furht, 2010; Mell & Grance, 2011; Sosinsky, 2011). Service models describe *what* a consumer gets from the service (software, platform, or infrastructure as a service – SaaS, PaaS, and IaaS); deployment models characterize *how* the service is delivered (publicly for everyone or privately, just for the costumer). And, to make things even more complicated, many entities are included on both sides, provider and customer. Providers may deliver the service (a software) and may be a service customer at the same time (e.g. when the programmer of a software as a service is using the platform as a service) (Habib, Ries, & Mühlhauser, 2011). The complete picture of the definitional framework of Cloud Computing services is depicted in Figure 1.

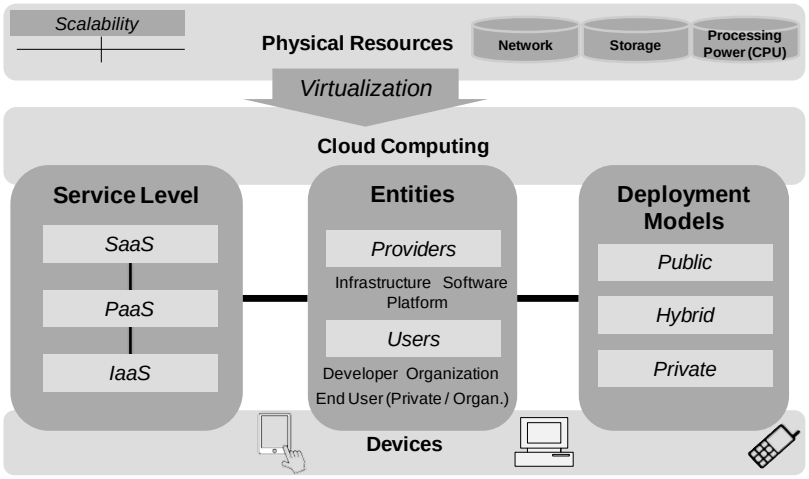

Figure 1. Cloud computing definitional framework, adapted from Furht (2010) and Sosinsky (2011)

Trust and Cloud Computing

Like many terms from everyday language, trust is used in science across many disciplines (Marsh, 1994). Each scientific discipline agrees on the importance of trust, but has its own way to define it, to built theories or models, and to apply it to research (Tschannen-Moran & Hoy, 2000). Following organizational and management studies trust

is the willingness of a person (the trustor) to be depend on another entity (the trustee) (McKnight et al., 1998) Doing so, the trustor becomes vulnerable (Mayer et al., 1995). Trust occurs voluntarily and involves perceived uncertainty and perceived risk on the side of the trustor and moral agency on the side of the trustee. In this context trust evolved to reduce complexity in everyday life (Luhmann, 1968).

Aside from that, Cloud Computing is a new piece of ICT. Though technology is implemented to promote the life of users, many users behave skeptically towards these innovations since new technologies tend to be more opaque, complex, and lead to a loss of controllability (Lee & See, 2004). This impenetrability of new technologies can lead to peoples' skepticism against it. Trust in technology may work as one way to reduce this skepticism.

Compared to any traditional form of offline or local computing (i.e. client-based computing) cloud computing leads to a decline of control over the data (Cavoukian, 2008). Therefore security and privacy risks, like data leakage, mass surveillance, or data loss, increase (Pearson, 2013). These risks increase in relation to the service that is delivered by the cloud provider. Software as a service entails more risks than platform as a service and platform as a service goes along with more risks compared to infrastructure as a service. The more service is provided, the less control remains on the user's side. If risks increase, non-acceptance and a non-usage of cloud computing might increase, too.

Taken together, there are three ways to respond to this widening lack of control in cloud computing technologies and risks that accompany them. First, we can try to mitigate risks that come with cloud computing services by, for example, not using these services. Technology-based risk mitigation is often closely linked to encryption (Ryan, 2013) in order to increase safety and security (Pearson, 2013). Second, we can build control systems that take care of increasing risks. There are several ways to do that. On the one hand one can establish policy-based control systems like service level agreements, quality of service, audits, and accreditation (Huang & Nicol, 2013). On the other hand reputation-based systems like measuring and ratings are often implemented (Habib, Hauke, Ries, & Mühlhäuser, 2012). Third, one can increase the user's trust in the cloud.

MODEL AND HYPOTHESES

Modeling trust empirically is crucial to validate the ideas about the underlying mechanisms of trust. In literature there are many ideas about the emergence of trust in cloud computing. Hence the present paper integrates existing models to unravel trust in the cloud. The emerging research model follows on investigations using the Technology Acceptance Model[1] (TAM) to explain the intention to (not) use a cloud-based information system (Behrend, Wiebe, London, & Johnson, 2011; Wu, Lan, & Lee, 2013). In addition, the present research model integrates assumptions that highlight the switching behavior from a client- to a cloud-based system using migration or switching approaches (Bhattacherjee & Park, 2013; Park & Ryoo, 2013). Yet, all models suggest factors that are important for the acceptance of cloud computing services. However, trust has never been used in those models to analyze the (non-)usage of cloud-based systems. Therefore this paper addresses trust in cloud computing by building a research model that integrates and expands previous works.

The proposed research model can be seen in Figure 2. On the left-hand side of the model, important trust antecedents as to perceived privacy and security are included. This part is very important because trust in cloud computing and online storage is often referred to privacy and security issues. Reputation is another salient part of trust. On the bottom of Figure 2, interpersonal control variables like personal innovativeness and disposition to trust are included.

On the top of the research model, classical building blocks from TAM like Perceived Ease of Use (PEOU) and Perceived Usefulness (PU) are shown. The behavioral outcome variable (usage of the service) is arranged on the right side of Figure 2 and defined by the frequency of use, that is the use in depth (with how many devices) and in width (how often are several functions used). In the present research model, trust has a major role as it can change

[1] The TAM is a model from information systems research dealing with the question why people use or not use a technology (King & He, 2006). TAM postulates two beliefs leading to the intention to use (not use) a particular system, Perceived Ease of Use (PEOU) and Perceived Usefulness (PU) (Davis & Venkatesh, 1996). The model argues that the intention to use a system may affect the actual usage of the system.

the relationships between essential antecedents of cloud computing usage (privacy, security and reputation), usability issues (usefulness and ease of use) as well as interpersonal characteristics (disposition to trust and personal innovativeness). This prominent role of trust discriminates the present research model from other models in the domain. In the following sections the hypothesis concerning each of these factors are derived from literature.

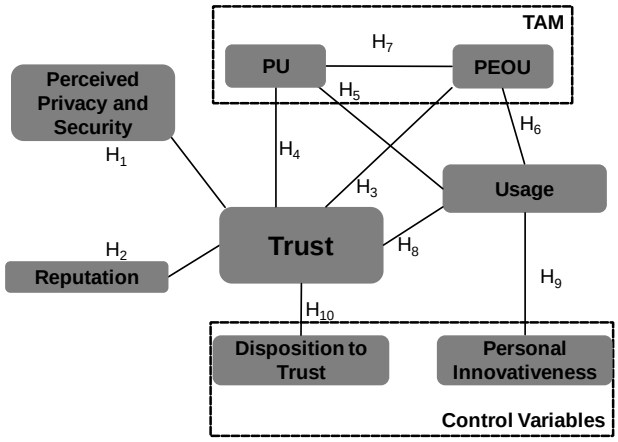

Figure 2: Proposed research model and hypotheses (PEOU: perceived ease of use, PU: perceived usefulness)

Impact of Perceived Privacy and Security on Trust

The fast growing field of information and communication technologies makes high capacity data processing more complex and therefore less transparent and intelligible to most users. Privacy and security are both important aspects when it comes to entrust your data to another entity. Warren and Brandeis (1890) defined privacy as *the right to be let alone*. It means that no one may determine the collection or disclosure of personal information except the person him- or herself (Cavoukian, 2008).

Similar to privacy, security in the cloud deals with the protection against unauthorized access or data loss. This is connected with all technical aspects like the integrity, confidentiality, authentication, and non-recognition of relationships (Casaló, Flavián, & Guinalíu, 2007).

Both aspects, privacy and security, top the lists of users' concerns towards the cloud (Pearson, 2013; Uusitalo, Karppinen, Juhola, & Savola, 2010). The individual need for privacy and security is therefore closely related to trust. Users often apply perceived privacy and security to assess the trustworthiness of a service. If privacy and security regulations are lower than user's demands, they might not use the service since he or she thinks it is not trustworthy enough.

For example, studies from e-commerce have shown that privacy and security are both influencing the trust in an e-vendor. Chellappa and Pavlou (2002) found that information security is directly connected to trust in an e-vendor. They found encryption, protection, verification, and authentication being associated with trust. Chen and Dibb (2010) reported a significant increase in trust for websites with better security and privacy assurances, e.g. secure transaction mechanisms and presence of trusted third party signs. Yoon (2002) describes trust as mediator between security and the intention to purchase online. Based on these findings, the first hypothesis is:

> *H_1: Perceived privacy and security have a positive impact on the user's trust in a cloud computing service.*

Impact of Reputation on Trust

As it can be seen in everyday life, gossip is sometimes half the truth. Word-of-mouth of friends or family are often taken in account when judging an entity, especially if we don't have any experience with something we have to interact with (Jarvenpaa, Tractinsky, & Saarinen, 2006). For example Ba and Pavlou (2002) found that more positive ratings in seller feedbacks on eBay have a positive influence on the buyers level of trust. However negative

feedback has an even stronger negative impact on trust ratings than positive feedback boosts them. Walczuch and Lundgren (2004) spotted an positive effect of several ways of perceived reputation on the trust in an e-vendor. They found positive word-of-mouth, friends and relatives, neutral sources, and marketer dominated sources to have an impact on trust. Related to these findings from online trust it is hypothesized:

H_2: Reputation is positively affecting trust in a cloud computing service.

Technology Acceptance Model Variables and Trust

Several models incorporate parts from the TAM and trust (Benamati, Fuller, Serva, & Baroudi, 2010; Gefen, Karahanna, & Straub, 2003; Wu & Chen, 2005). Pavlou (2003), as well as Benamati and colleagues (2010) report a strong relationship between both, perceived ease of use, perceived usefulness, and trust. Relating to this evidence the two hypotheses are proposed:

H_3: The level of trust in a cloud computing service affects the perceived ease of use of the service.
H_4: The level of trust in a cloud computing service affects the perceived usefulness of the service.

As known from empirical findings of TAM research, perceived usefulness and perceived ease of use also affect the usage of a technology or system (Turner, Kitchenham, Brereton, Charters, & Budgen, 2010). Wu and colleagues (2013) found that perceived ease of use plays a crucial role for the acceptance of cloud services in university. Perceived usefulness was found to foster the usage of a university-related cloud service. Bhattacherjee and Park (2013) described that the relative usefulness (similar to perceived usefulness in TAM) enhances the migration of users to cloud services. Additionally, most investigations using TAM report effects of perceived ease of use on perceived usefulness (Pavlou, 2003; Wu & Chen, 2005). Summing up, easy-to-use technologies lead to a more efficient way of interaction. Hence perceived usefulness and ease of use affect technology usage. This summary leads to the following assumptions:

H_5: Perceived usefulness is positively related to the actual usage of a cloud computing service.
H_6: Perceived ease of use is positively related to the actual usage of a cloud computing service.
H_7: Perceived ease of use is also positively related to the perceived usefulness of a cloud computing service.

Finally, trust is positively related to a trustful behavior, i.e. the usage of the trusted system (Chang & Fang, 2013; Pavlou, Liang, & Xue, 2007; Pavlou, 2003):

H_8: The level of trust in a cloud computing service is positively related to the actual usage of the service.

Control Variables

In the present research model (see Figure 2) personal innovativeness and the disposition to trust are included as control variables. With respect to the personal innovativeness, a high level of personal innovativeness is closely related to technophilia and curiosity towards technology (Venkatesh, Morris, Davis, & Davis, 2003). It means that if someone has a huge level of personal innovativeness, he is more likely to use a system, no matter how much he trusts it (Park & Ryoo, 2013). Regarding the disposition to trust it is well known that it affects all kinds of trust like trust in people, things, technology, or systems (Gefen et al., 2003; Gefen & Straub, 2004; Gefen, 2000). Based on this evidence the following hypotheses can be framed:

H_9: A high level of personal innovativeness is positively related to the use of a cloud computing service.
H_{10}: The disposition to trust is positively related to trust in a cloud computing service.

EMPIRICAL SURVEY

Context, Sample, and Procedure

Respondents were users and non-users of the cloud storage service Dropbox used for the study. Dropbox was used since it is a very popular tool to share data and materials in Germany and worldwide. Furthermore, Dropbox is available for free (2GB) and can be installed very easily on desktop PCs as well as mobile devices (dropbox.com, last visit: 28.02.2014).

135 students from the Technische Universität Berlin were surveyed. Two participants were excluded because of missing values. Therefore the final sample comprised of 47 female and 86 male students. They were on average M = 24.86 years old (SD = 5.80) and studied for M = 4.77 semesters (SD = 2.35). Most respondents were enrolled in engineering studies (45.30 %), psychology (19.70 %), and computer science (12.80 %), completed by humanities and medicine (12.80 %). The majority of 108 students (80.00 %) used Dropbox. Only 27 students (20.00 %) stated that they didn't use the service.

All respondents completed a paper-and-pencil questionnaire. The questionnaire was in German and comprised of several item batteries operationalizing the aforementioned constructs (see Fig.2), demographical questions, and questions about the usage of Dropbox and other ways to store data (see appendix A.1 for a translated version of the instrument). The completion of the questionnaire took about 10 minutes. Subjects participated voluntarily.

Variable Definition

To assess model constructs established scales from studies involving TAM, switching behavior, and online trust (see Table 1 for references and appendix A.1 for item wordings) were used. Due to the length of the final questionnaire, some items from the original scales were dropped.

Results

SmartPLS and SPSS were used to build a structural model. Partial Linear Squares (PLS) models were employed, since they reduce the chance of type II errors in case of misspecification (Vinzi, Chin, Henseler, & Wang, 2010). Furthermore they can be used with smaller sample sizes and they unravel even small effects. The analysis of the model quality was conducted in two steps. First, reliabilities (Cronbach's alpha, α) were calculated. They ranged from good ($.70 \leq \alpha < .80$) to very good ($.80 \leq \alpha$) reliability scores (see Table 1). Considerable cross-loadings were not found (see Appendix, Table A.2). In a second step the average variance extracted (AVE) was assessed. All scales passed the criterion of an AVE of more than 0.50 (Vinzi et al., 2010).

Table 1: Applied scales and their reliability (Cronbach's alpha) in the present survey

Measure	Reference	α	AVE
Privacy & Security	Casálo, et al., 2007	0.92	0.57
Reputation	Casálo, et al., 2007	0.81	0.73
Trust	Corritore et al., 2005	0.89	0.72
Perceived Ease of Use	Davis & Venkatesh, 1996	0.90	0.78
Perceived Usefulness	Davis & Venkatesh, 1996	0.90	0.77
Disposition to Trust	Beierlein et al., 2012	0.81	0.72
Personal Innovativeness	Agarwal & Prasad, 1998	0.88	0.74

Since requirements were met, a PLS analysis was conducted using bootstrapping for inference statistics. The results of the PLS analysis are displayed in Figure 3. Six linkages of the models had significant, four linkages had non-significant path coefficients. Large path weights were obtained for privacy and security on trust (H_1) and for most of the TAM variables (H_3-H_7). Trust (H_8) and perceived ease of use (H_6) had no effects on usage behavior. Trust had no effect on perceived ease of use (H_3), too. The influence of the disposition to trust on trust in Dropbox was very low and non-significant (H_{10}).

Perceived Privacy and Security as well as reputation explained 69.50 % of the variance of trust in Dropbox. The proportion of total variation of the usage behavior was explained to 40.40 % by perceived usefulness, perceived ease of use, and personal innovativeness (H_9).

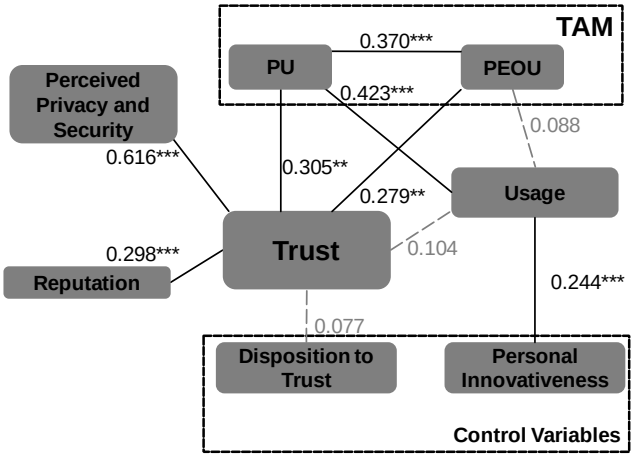

Figure 3: Results of the PLS model, (** p < 0.01, *** p < 0.001), dashed, grey lines indicate non-significant path coefficients

DISCUSSION

This investigation is one of the first attempts to empirically analyze trust in cloud computing. The theoretical framework of the empirical model was derived from studies of trust and acceptance of online information systems, like e-vendors, information websites, or e-government platforms. To some parts the present work replicated results and underlying assumptions of previous studies. For example the components from TAM showed their typical pattern in the research model of this paper. Perceived usefulness had an impact on the use of Dropbox (H_5). Typically, perceived ease of use had an influence on perceived usefulness (H_7). The replication of this linkage in the present survey reflects the fundamental, theoretical principles of TAM. However, perceived ease of use had no direct influence on the usage of Dropbox (H_6), maybe perceived usefulness works as a moderator between perceived ease of use and actual usage behavior.

The importance of privacy and security as antecedents of trust in cloud computing was underlined in the present investigation as well (H_1). Especially for Dropbox, privacy and security issues are discussed due to mass surveillance disclosure (see articles related to PRISM and TEMPORA) and security flaws in the short history of the system. Therefore privacy and security remain key issues for people. In the field of online data storage, reputation is another important issue. Since many decisions to use a system are influenced by personal recommendation and feedback from users, reputation is important for trust in cloud computing services like Dropbox (H_2). This knowledge can be transferred to marketing to create good word-of-mouth and reputation in the online community.

However, in the field of trust many results counteract researcher's expectations. For example in the present study, no effects were found for trust and Dropbox usage (H_8), that means there was no direct connection between trust and the outcome behavior. Maybe some mediators play a crucial role here. On the one hand, trust maybe not the key factor to use Dropbox. Based on the present data, perceived usefulness was the best predictor of user behavior. On

the other hand, trust was mediated by perceived usefulness in the model. Social influences like peer-group pressure may moderate the effect of trust on behavior as well. In case students ask another student to use Dropbox to collaborate in a group work one may have no alternative. This combination can lead to low trust levels even though a person uses Dropbox regularly. Additionally, the disposition to trust did not affect trust in Dropbox in this study (H_{10}). This result is puzzling to some degree. Maybe assessing trust in Dropbox is too concrete so that trust is strongly affected by other characteristics of the artifact and not related to an overall disposition anymore.

In contrast, the results regarding the effect of personal innovativeness agree with the hypothesis (H_9). The more technophile persons are, the more they use the system. The concept is independent from trust or the disposition to trust in the model (see cross-loadings in appendix A.2). Therefore, personal innovativeness seems to be an independent concept.

Shortcomings of the Survey Study

The study has several shortcomings that make it difficult to generalize the results. First, the respondents were students. Cloud computing is very present in the academic context (Mokhtar, Ali, Al-Sharafi, & Aborujilah, 2013). Students use cloud services in order to organize their studies and to collaborate with others. Furthermore, the young sample is more open to new technologies and receives higher education. This may lead to a high technology acceptance level, which is not representative for the average user. Second, the analyzed software as a service Dropbox is only covering a small part of the cloud computing framework. Different trusting and using patterns could be expected from other contexts of use, e.g. infrastructure or platform as a service. Third, social contexts were not analyzed at all. Future investigations should take a look at social influences, like social norms or the influence of peers and friends, to be able to analyze their moderating influence on the interaction of trust and system usage.

Implications for Theory

The present study shows that trust is an integral part of information system acceptance and use. Therefore, theories and models should incorporate trust and existing models of technology acceptance and technology use (like TAM, migration models, Herzberg models, switching models, etc.). Trust can be used to enrich these models in order to better understand user behavior. The presented research model can be used to analyze the usage of an incumbent or the switching to a new system whilst taking trust into account. Trust is an important factor hindering the acceptance of a system. In addition it mitigates the efficient use of a system with being less efficient when it is not trusted (Gefen, 2000).

Another theoretical extension of existing approaches can be seen in the transfer of existing models on a new information system, cloud computing. Applying the models on a cloud service is a relatively undiscovered field of information system research. On the one hand their application in the new domain provides new insights to the way people use and feel about the cloud technology. On the other hand, it shows that existing approaches can be helpful to some parts to understand new technologies.

Implications for Practical Applications

The results of this study may be helpful for all entities and agents of the cloud computing framework, i.e. users, providers, programmers, and deciders in organizations. Providers may wish to increase the use of their cloud services. To accomplish that goal, several ways may be applicable based on the research model. Providers can increase the perceived usability by looking at the target group of their service to address their needs and make the service useful for them. In organizations, training may be helpful to communicate to organizational users what the service provides for a more efficient and effective work. These trainings should highlight the advantages of cloud-based solutions. In the same step, issues related to privacy, security, and trust should be addressed, too. Especially bad reputations and word-of-mouth from private or public sources may lead to a lack of trust and suspicion, even though it is without any reason. Providers and organizational deciders should communicate privacy and security issues in a transparent and open way. Trainings and transparency may even help the user to face the complexity of cloud computing services and work more efficiently. This, in turn, leads to more satisfied users.

Conclusion and Outlook

The investigation adds more empirical insights to the importance and underlying mechanisms of trust and technology use. First, it enriches existing frameworks with trust. Second, it transfers these enriched frameworks on a cloud-based technology taking the end-user's perspective. The integration of these frameworks shows several pathways of technology acceptance (TAM) and trust. Key findings are the vital importance of security and privacy issues for the trust in cloud services. The research model indicates no direct relationship from trust to the actual system usage. This speaks for the social influence of others, which leads one to use a system though one does not trust it. Future investigations should take a closer look at this possible mediator variable. Furthermore, some other antecedents of trust might be scrutinized, like perceived risk, aesthetics of the interface, or antecedents of the provider like integrity, ability, and benevolence. If one looks ahead, the pervasiveness and complexity of cloud-based information and communication systems is certainly increasing. In order to deal with this complexity, trust in new technologies should be monitored to provide trustworthy and transparent technologies to responsible users.

References

Agarwal, R., & Prasad, J. (1998). A conceptual and operational definition of personal innovativeness in the domain of information technology. *Information Systems Research*, *9*(2), 204–215.

Ba, S., & Pavlou, P. A. (2002). Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior. *MIS Quarterly*, *26*(3), 243–268.

Behrend, T. S., Wiebe, E. N., London, J. E., & Johnson, E. C. (2011). Cloud computing adoption and usage in community colleges. *Behaviour & Information Technology*, *30*(2), 231–240. doi:10.1080/0144929X.2010.489118

Beierlein, C., Kemper, C. J., Kovaleva, A., & Rammstedt, B. (2012). Kurzskala zur Messung des zwischenmenschlichen Vertrauens: Die Kurzskala Interpersonales Vertrauen. *GESIS - Working Papers*, (22). Retrieved from http://www.gesis.org/uploads/media/KUSIV3_Workingpaper.pdf

Benamati, J., Fuller, M. A., Serva, M. A., & Baroudi, J. (2010). Clarifying the Integration of Trust and TAM in E-Commerce Environments: Implications for Systems Design and Management. *IEEE Transactions on Engineering Management*, *57*(3), 380–393. doi:10.1109/TEM.2009.2023111

Bhattacherjee, A., & Park, S. C. (2013). Why end-users move to the cloud: a migration-theoretic analysis. *European Journal of Information Systems*, 1–16.

Casaló, L. V., Flavián, C., & Guinalíu, M. (2007). The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review*, *31*(5), 583–603. doi:10.1108/14684520710832315

Cavoukian, A. (2008). Privacy in the clouds. *Identity in the Information Society*, *1*(1), 89–108. doi:10.1007/s12394-008-0005-z

Chang, Y.-S., & Fang, S.-R. (2013). Antecedents and Distinctions Between Online Trust and Distrust: Predicting High- and Low-Risk Internet Behaviors. *Journal of Electronic Commerce Research*, *14*(2). Retrieved from http://www.csulb.edu/web/journals/jecr/issues/20132/paper2.pdf

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, *15*(5/6), 358–368. doi:10.1108/09576050210447046

Chen, J., & Dibb, S. (2010). Consumer trust in the online retail context: Exploring the antecedents and consequences. *Psychology and Marketing*, *27*(4), 323–346. doi:10.1002/mar.20334

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, *58*(6), 737–758. doi:10.1016/S1071-5819(03)00041-7

Davis, F. D., & Venkatesh, V. (1996). A critical assessment of potential measurement biases in the technology acceptance model: three experiments. *International Journal of Human-Computer Studies*, *45*(1), 19–45.

Gefen, D. (2000). E-commerce: the role of familiarity and trust. *Omega*, *28*(6), 725–737. doi:10.1016/S0305-0483(00)00021-9

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Inexperience and experience with online stores: The importance of TAM and trust. *IEEE Transactions on Engineering Management*, *50*(3), 307–321. doi:10.1109/TEM.2003.817277

Gefen, D., & Straub, D. W. (2004). Consumer trust in B2C e-Commerce and the importance of social presence: experiments in e-Products and e-Services. *Omega*, *32*(6), 407–424. doi:10.1016/j.omega.2004.01.006

Habib, S. M., Hauke, S., Ries, S., & Mühlhäuser, M. (2012). Trust as a facilitator in cloud computing: a survey. *Journal of Cloud Computing*, *1*(1), 1–18.

Habib, S. M., Ries, S., & Mühlhauser, M. (2011). Towards a trust management system for cloud computing. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on* (pp. 933–939). Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6120922

Huang, J., & Nicol, D. M. (2013). Trust mechanisms for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, *2*(1), 9.

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (2006). Consumer Trust in an Internet Store: A Cross-Cultural Validation. *Journal of Computer-Mediated Communication*, *5*(2), 0–0. doi:10.1111/j.1083-6101.1999.tb00337.x

Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *46*(1), 50–80.

Mokhtar, S. A., Ali, S. H. S., Al-Sharafi, A., & Aborujilah, A. (2013). Cloud computing in academic institutions. In *Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication* (p. 2). Retrieved from http://dl.acm.org/citation.cfm?id=2448558

Onwubiko, C. (2010). Security Issues to Cloud Computing. In N. Antonopoulos & L. Gillam (Eds.), *Cloud Computing* (pp. 271–288). London: Springer. Retrieved from http://link.springer.com/10.1007/978-1-84996-241-4_16

Park, S. C., & Ryoo, S. Y. (2013). An empirical investigation of end-users' switching toward cloud computing: A two factor theory perspective. *Computers in Human Behavior*, *29*(1), 160–170. doi:10.1016/j.chb.2012.07.032

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), 101–134.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective. *MIS Quarterly*, *31*(1), 105–136.

Pearson, S. (2013). Privacy, Security and Trust in Cloud Computing. In S. Pearson & G. Yee (Eds.), *Privacy and Security for Cloud Computing* (pp. 3–42). Heidelberg: Springer.

Ryan, M. D. (2013). Cloud computing security: The scientific challenge, and a survey of solutions. *Journal of Systems and Software*, *86*(9), 2263–2268. doi:10.1016/j.jss.2012.12.025

Turner, M., Kitchenham, B., Brereton, P., Charters, S., & Budgen, D. (2010). Does the technology acceptance model predict actual use? A systematic literature review. *Information and Software Technology*, *52*(5), 463–479. doi:10.1016/j.infsof.2009.11.005

Uusitalo, I., Karppinen, K., Juhola, A., & Savola, R. (2010). Trust and Cloud Services - An Interview Study (pp. 712–720). Presented at the IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), Indianapolis, IN: IEEE. doi:10.1109/CloudCom.2010.41

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425–478.

Vinzi, V. E., Chin, W., Henseler, J., & Wang, H. (Eds.). (2010). *Handbook of partial least squares: Concepts, methods and applications*. Heidelberg: Springer.

Walczuch, R., & Lundgren, H. (2004). Psychological antecedents of institution-based consumer trust in e-retailing. *Information & Management*, *42*(1), 159–177. doi:10.1016/j.im.2003.12.009

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220.

Wu, I.-L., & Chen, J.-L. (2005). An extension of Trust and TAM model with TPB in the initial adoption of on-line tax: An empirical study. *International Journal of Human-Computer Studies*, *62*(6), 784–808. doi:10.1016/j.ijhcs.2005.03.003

Wu, W.-W., Lan, L. W., & Lee, Y.-T. (2013). Factors hindering acceptance of using cloud services in university: a case study. *The Electronic Library*, *31*(1), 84–98. doi:10.1108/02640471311299155

Yoon, S.-J. (2002). The antecedents and consequences of trust in online-purchase decisions. *Journal of Interactive Marketing*, *16*(2), 47–63. doi:10.1002/dir.10008

APPENDIX

Table A. 1: Model constructs and item wording

Construct	Item No.	Item wording
Privacy and Security (Casaló u. a., 2007)	P&S 1	I think Dropbox shows concern for the privacy of its users.
	P&S 2	I feel safe when I send personal information to this web site.
	P&S 3	I think Dropbox abides by personal data protection laws.
	P&S 4	I think Dropbox only collects user personal data that are necessary for its activity.
	P&S 5	I think Dropbox respects the user's rights when obtaining personal information.
	P&S 6	I think that Dropbox will not provide my personal information to other companies without my consent.
	P&S 7	I think Dropbox has mechanisms to ensure the safe transmission of its users' information.
	P&S 8	I think Dropbox shows great concern for the security of any transactions.
	P&S 9	When I send data to this web site, I am sure that they will not be intercepted by unauthorized third parties.
	P&S 10	I think Dropbox has sufficient technical capacity to ensure that the data I send cannot be modified by a third party.
	P&S 11	Overall I'm sure Dropbox is a safe place for my data.
Reputation (Casaló u. a., 2007)	REP 1	Dropbox has a good reputation.
	REP 2	Dropbox has a good reputation compared to other rival web sites.
	REP 3	Dropbox has a reputation for offering good products and services.
Trust (Corritore, Kracher, & Wiedenbeck, 2003)	Trust 1	I think Dropbox is trustworthy.
	Trust 2	I believe Dropbox will not act in a way that harms me.
	Trust 3	I trust Dropbox.
Perceived Ease of Use (Davis & Venkatesh, 1996)	PEOU 1	The interaction with Dropbox is clear and understandable.
	PEOU 2	Interacting with Dropbox does not require a lot of my mental effort.
	PEOU 3	I find Dropbox easy to use.
	PEOU 4	I find it easy to get Dropbox to do what I want it to do.
Perceived Usefulness (Davis & Venkatesh, 1996)	PU 1	Using Dropbox improves my performance.
	PU 2	Using Dropbox increases my productivity.
	PU 3	Using Dropbox enhances my effectiveness.
	PU 4	I find Dropbox useful.
Disposition to Trust (Beierlein, Kemper, Kovaleva, & Rammstedt, 2012)	DT 1	I am convinced, all people have good intentions.
	DT 2	Nowadays you can't rely on anybody.*
	DT 3	In general, you can trust people,
Perceived Innovativeness (Agarwal & Prasad, 1998)	PI 1	If I heard about a new information technology, I would look for ways to experiment with it.
	PI 2	Among my peers, I am usually the first to try out new information technologies
	PI 3	In general. I am hesitant to try out new information technologies.*
	PI 4	I like to experiment with new information technologies.
Dropbox Use (Calculated from demographics)	USE 1	How often do you use the following functions of Dropbox? (Mean)
	USE 2	Which devices do you synchronize with Dropbox? (Percentage of devices)

*Note: * reverse scaled item*

Table A.2: PLS item factor and cross loadings

Item No.	P&S	REP	Trust	PEOU	PU	DT	PI	USE
P&S 1	0.7378	0.3918	0.5509	0.1239	0.2821	0.0256	0.0436	0.1604
P&S 2	0.7502	0.3902	0.6056	0.2015	0.2137	0.1022	0.0172	0.1931
P&S 3	0.7939	0.4270	0.6072	0.0771	0.1083	0.1630	-0.0028	0.1526
P&S 4	0.6415	0.2044	0.3451	0.0802	0.2227	0.0376	0.0571	0.1416
P&S 5	0.7908	0.4260	0.6293	0.0711	0.1951	0.1834	0.0777	0.1653
P&S 6	0.7804	0.4032	0.6029	0.1486	0.2541	0.0641	0.0563	0.2761
P&S 7	0.7352	0.3949	0.5971	0.1251	0.2529	0.1193	0.1417	0.1651
P&S 8	0.7587	0.4596	0.6271	0.1272	0.2493	0.1829	0.1102	0.1974
P&S 9	0.6677	0.3048	0.4654	0.0767	0.3432	0.1664	-0.0014	0.2164
P&S 10	0.8400	0.4386	0.7094	0.0202	0.2250	0.2095	0.0730	0.2080
P&S 11	0.7798	0.4834	0.6785	0.1502	0.3143	0.1752	0.0303	0.2599
REP 1	0.4819	0.8829	0.6072	0.0969	0.2548	0.1052	-0.0080	0.2154
REP 2	0.3917	0.8549	0.5011	0.2218	0.3604	0.2010	0.1433	0.2486
REP 3	0.4816	0.8172	0.5196	0.0535	0.2663	0.2043	0.1112	0.2686
Trust 1	0.7856	0.5798	0.9121	0.2550	0.2631	0.1702	0.0851	0.1790
Trust 2	0.4832	0.4610	0.7227	0.2168	0.2052	0.1668	0.1389	0.2244
Trust 3	0.7042	0.5816	0.8990	0.2395	0.2993	0.2800	0.0563	0.3170
PEOU 1	0.1433	0.1805	0.2637	0.9199	0.4002	0.0859	0.3031	0.3591
PEOU 2	0.1613	0.0806	0.2287	0.7571	0.3797	0.0979	0.2412	0.3665
PEOU 3	0.1194	0.1339	0.2626	0.9349	0.3924	0.0184	0.2700	0.3105
PEOU 4	0.0721	0.0976	0.2197	0.9047	0.3124	0.0662	0.2979	0.2645
PU 1	0.2825	0.3202	0.2525	0.3084	0.8909	-0.0178	0.3147	0.5332
PU 2	0.2803	0.2436	0.2401	0.3103	0.8907	0.0607	0.2952	0.4187
PU 3	0.2924	0.2203	0.2236	0.3007	0.9209	-0.0415	0.2320	0.4459
PU 4	0.2537	0.3708	0.3235	0.5168	0.8054	0.1303	0.2476	0.5521
DT 1	0.2453	0.2028	0.2556	0.0519	0.0553	0.9050	0.1744	0.2239
DT 2	0.0874	0.1519	0.1858	0.0559	0.0491	0.8066	0.1551	0.1595
DT 3	0.0837	0.1278	0.1646	0.0988	0.0020	0.8357	0.1800	0.1432
PI 1	0.0142	0.0474	0.0205	0.2897	0.3018	0.1230	0.9092	0.3978
PI 2	0.0631	0.0776	0.1110	0.2673	0.2878	0.1942	0.8976	0.4173
PI 3	0.0311	0.0739	0.0584	0.1500	0.1106	0.1691	0.7524	0.1907
PI 4	0.1420	0.1173	0.1635	0.3395	0.3082	0.2089	0.8703	0.3484
USE 1	0.2070	0.2902	0.2288	0.3375	0.5319	0.1444	0.4080	0.8891
USE 2	0.2036	0.1173	0.2166	0.2296	0.3153	0.2110	0.1962	0.6348

Abbreviations: P& S: Privacy and Security; REP: Reputation; PEOU: Perceived Ease of Use; PU: Perceived Usefulness; DT: Disposition to Trust; PI: Personal Innovativeness; USE: Usage of Dropbox