TRUST TRANSITIVITY AND TRUST PROPAGATION IN CLOUD COMPUTING ECOSYSTEMS

Research Paper

Adelmeyer, Michael, Osnabrück University, Osnabrück, Germany, michael.adelmeyer@uni-osnabrueck.de

Walterbusch, Marc, Osnabrück University, Osnabrück, Germany, marc.walterbusch@uni-osnabrueck.de

Biermanski, Peter, Osnabrück University, Osnabrück, Germany, pbiermanski@uni-osnabrueck.de

Teuteberg, Frank, Osnabrück University, Osnabrück, Germany, frank.teuteberg@uni-osnabrueck.de

Abstract

Due to security and privacy concerns, trust is a vital facilitator of successful business relationships in cloud computing ecosystems. This is especially true when customers obtain adapted services built on third-party cloud services. In this case, customers are no longer interacting with service providers directly. Instead, they rely on mediators and, thus, are dependent on the mediators' choices and judgement. Hence, we analyze the role of trust transitivity and propagation – the derivation of a certain amount of trust from a trust relationship with a directly known party – between individual customers and mediators as well as service providers in an online experiment. The results reveal no significant evidence for trust transitivity (complete propagation of the level of trust between the actors) in cloud computing trust chains. Rather, individual customers' trust is propagated between mediators and cloud service providers. This evidence is important for providers, as they could mitigate direct trust issues by providing services indirectly. Further, mediators should be aware that trust and consequently the usage behavior of individual customers can be affected by incidents which are caused by providers. For science, this understanding is vital to further examine and understand the role of trust in cloud adoption and usage.

Keywords: Cloud Computing, Trust, Transitivity, Propagation, Usage Intention, Online Experiment.

1 Introduction

In recent years, cloud computing (CC) has gained sweeping attention, since it allows for rapid provisioning of scalable computing resources, which can be used and combined for encapsulation of individual services (Armbrust et al., 2010). The decision to adopt and to use cloud computing services (CCS) or to outsource existing software, hardware or systems into the cloud is also influenced by subjective factors such as trust (Lansing and Sunyaev, 2016; Pearson, 2013), that can hinder the adoption (Chu et al., 2013; Géczy et al., 2012). In the CC market, a customer or CCS user holds the position of the trustor, who in turn places trust in a cloud provider, the trustee (Mayer et al., 1995). However, in addition to customers and providers, other stakeholders emerged in the CC market, such as mediators (Böhm et al., 2010; Leimeister et al., 2010; Walterbusch et al., 2013). Mediators adapt existing CCS on the basis of which they offer customized or further developed cloud services (Leimeister et al., 2010). For example, the cloud-filehoster Dropbox (mediator) formerly used Amazon Web Services' cloud (provider) as basic service for the storage of customer data (Drago et al., 2012). This nested network of cloud services and providers offered in impersonal marketplaces is commonly referred to as *cloud computing ecosystem* (Lansing and Sunyaev, 2016; Pearson, 2013; Böhm et al., 2010). As such constellations entail additional dependencies and relationships (Lansing and Sunyaev, 2016), it is necessary to extend the trust chain to other involved actors within CC ecosystems. From a customer's perspective at the end of a trust chain, the traditional outsourcing model of direct service provisioning is replaced by a web of dependencies from different providers and interjacent mediators (Floerecke and Lehner, 2016). Equally, a mediator is dependent on basic service providers. Thus, incidents at or actions by certain actors (e.g., unavailability of a provider) have an influence on the trust and related business relationships of other actors (i.e., customers and mediators). In this context, it is mandatory to understand whether such incidents affect the trust relationship between a customer and a mediator and to which extent a customer's direct trust in a provider differs from the indirect trust via a mediator.

In such three-part trust chains, the transfer of trust from a directly known entity to an indirectly known entity is referred to as *transitivity* or *propagation* (Jøsang and Pope, 2005). Transitivity only occurs in case of complete propagation, which is sometimes confused in literature (Sherchan et al., 2013). Existing research in CC mainly focuses on direct trust relationships, e.g., between providers and customers or in the technology itself (Lansing and Sunyaev, 2016; Walterbusch et al., 2013). Rather, empirical evidence on transitivity and propagation of trust along the chain from customers to cloud providers (Singh and Chand, 2014; Pearson, 2013) is still missing, although the partly opaque CC trust chain differs from other markets and traditional outsourcing with direct service provisioning (Lansing and Sunyaev, 2016). Due to the immense size and complexity of cloud computing ecosystems and given the fact that customers are often unaware of which actor provides what service component (Floerecke and Lehner, 2016), there is an urgent need to explore trust transitivity and propagation in cloud ecosystems as well as their impact on customers' decisions to adapt or to use cloud solutions of certain actors. Our study aims at investigating this gap by means of a vignette-based online experiment. Given the opacity of cloud environments and customers' frequent unawareness of the existence of third-party actors, surveys or quasi-experiments are not suitable. We examine both (i) the presence of a mediator and (ii) incidents affecting different actors (provider or mediator) and their impact on individual customers' trust at a functional (trust in the capabilities of providers) and a referral level (trust in the ability of mediators to adequately select a provider). We address the following research questions (RQ):

RQ1: Is trust between a customer, mediator and service provider in cloud ecosystems transitive?

RQ2: How do incidents at providers and mediators in cloud ecosystems affect individual end customers' levels of trust in the respective actors?

To answer these RQs, the study is structured as follows: first, the theoretical foundations are provided. Based on this, we develop corresponding hypotheses. Subsequently, we outline the research method including the experimental design, the operationalization of the experiment conditions and constructs as well as the data collection. Thereafter, the results of our online experiment are presented: first, we determine the impact of the experimental conditions; second, we evaluate the relationships of the constructs by means of a partial least squares (PLS) analysis. Our results indicate that trust in three-part trust chains is propagated between the actors. From a scientific point of view, this awareness is mandatory to further investigate trust relationships between interlinked parties in cloud ecosystems and their importance for cloud adoption and usage. In practice, our results draw the attention of mediators to the necessity of carefully selecting reliable providers to avoid a possible loss of trust.

2 Theoretical Foundations

2.1 Cloud Computing Ecosystem Actors

In the CC market, different types of actors emerged, disrupting the traditional value chain of IT service provisioning and forming a complex business ecosystem (Floerecke and Lehner, 2016). The main actors can be derived from the cloud service models: infrastructure, platform and application providers (Böhm et al., 2010; Leimeister et al., 2010). Those actors, who offer end products that are based on services of other providers, simultaneously hold two positions: customer and provider (Floerecke and

Lehner, 2016; Leimeister et al., 2010; Marston et al., 2011). For example, aggregators either integrate, customize or bundle existing basic services of third-party cloud providers and offer these newly created services directly to customers (Leimeister et al., 2010). This includes service integrators (providing a vertical connection of existing cloud services), service customizers (enhancing or adapting given external services) and service bundlers (offering bundles or compositions of cloud services without adding new functions) (Floerecke and Lehner, 2016). In case they simultaneously act as customer and provider in cloud ecosystems, aggregators as well as providers can be interpreted as hybrids (Floerecke and Lehner, 2016). The customer at the end of the value chain obtains the services either directly from a provider or indirectly via intermediaries (Leimeister et al., 2010). The hybrid and intermediary roles will hereinafter be summarized and referred to as mediators (Walterbusch et al., 2013; Keller and König, 2014). In this context, for example, Dropbox or Salesforce act as mediators, as they rely on basic cloud services provided by, e.g., Amazon Web Services (Floerecke and Lehner, 2016; Drago et al., 2012). In summary, it can be noted that the outsourcing into a cloud creates a large, nested network of trust relationships with multiple actors (Lansing and Sunyaev, 2016) (cf. Figure 1).

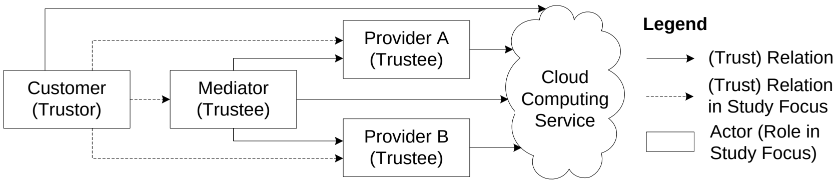


Figure 1. Simplified Trust Chain of Cloud Ecosystem Actors (Walterbusch et al., 2013).

In the course of this study, we focus on the following actors: (i) individual end customers, who obtain services either directly from a cloud provider or via a cloud mediator in a public cloud market, (ii) cloud mediators, who adapt services from cloud providers and offer these as own services and (iii) cloud providers, who provide services in the form of, e.g., Infrastructure as a Service (IaaS) for arbitrary actors (cf. Figure 1). In this context, trust is seen as a key factor for the successful adoption and use of cloud computing services (Lansing and Sunyaev, 2016; Noor et al., 2016; Garrison et al., 2012), since the customer must have a certain confidence in the provider's capabilities regarding the operation of the CCS or the underlying cloud infrastructure (Walterbusch et al., 2013). This comes especially true when outsourcing sensitive information into a cloud, like personal or critical company data (Pearson and Benameur, 2010; Ko et al., 2011; Zissis and Lekkas, 2012; Adelmeyer et al., 2016; Walterbusch et al., 2013). Trust in CC heavily depends on the selected deployment model, as control and governance over data are delegated to the cloud provider (Zissis and Lekkas, 2012). The customer (trustor) exposes himself to potential vulnerabilities in a unilateral dependency on the cloud provider (trustee) (Walter et al., 2014). The lack of direct personal interaction and the existence of mediators (trustee) even intensify the importance of trust in cloud ecosystems (Lansing and Sunyaev, 2016).

2.2 Trust Transitivity and Propagation

Mayer et al. (1995) define trust as "the willingness of a party to be vulnerable to the actions of another party 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 part". In addition to the consideration of the two parties trustor and trustee (two-part trust chain), trust relationships between multiple parties are investigated in the literature. Transferring trust from one entity to another is referred to as transitivity or propagation, whereby transitivity implies propagation but not vice versa (Sherchan et al., 2013). In general, trust is seen as non-transitive but rather propagative (Christianson and Harbison, 1996; Sherchan et al., 2013; Yu and Singh, 2000). As an example, we assume that party *A* trusts party *B* and party *B* trusts party *C*. In the case of transitivity, it could be concluded that party *A* (equally) trusts the indirectly known party *C* (Christianson and Harbison, 1996). In the case of propagation, party *A* can derive a certain degree of trust in an indirectly known party *C*, which is based on its trust in the intermediary party *B* as well as on the partially known relationship between party *B* and party *C* (three-part trust chain) (Sherchan et al., 2013). Thus, transitivity only occurs in the case of complete propagation.

In such relationships with three or more interlinked parties, different types of trust are to be distinguished. Trust can be either direct or indirect (through personal interactions or relationships with other social contacts) (Huang and Fox, 2006) as well as functional or referral (Jøsang and Pope, 2005; Jøsang et al., 2006). Since the trustor, in our example party *A*, directly knows and interacts with the trustee, party *B*, the trust relationship is direct. However, the trust relationship between party *A* and *C* is indirect, since *C* is only known indirectly via *B*. The customer's trust in the mediator's abilities to assess and to refer to a provider in the sense of the customer is addressed to as referral trust (RT). The trust in the abilities of a provider to perform a particular action relevant to the customer is referred to as functional trust (FT) (Jøsang and Pope, 2005; Jøsang et al., 2006). In a two-part trust chain, the customer's trust in a provider is designated as direct functional trust (DFT) and as indirect functional trust (IFT) in three-part trust chains. In the same context, Huang and Fox (2006) distinguish between "trust in belief" and "trust in performance", whereby only the trust of party *A* in the beliefs of party *B* is regarded as transitive. Moreover, according to Huang and Fox (2006), trust in belief is a special case of "recommendation trust". In this context, RT requires the existence of FT at the end of the trust path, which allows trust to become transitive (Jøsang et al., 2006; Jøsang and Pope, 2005) (cf. Figure 2).

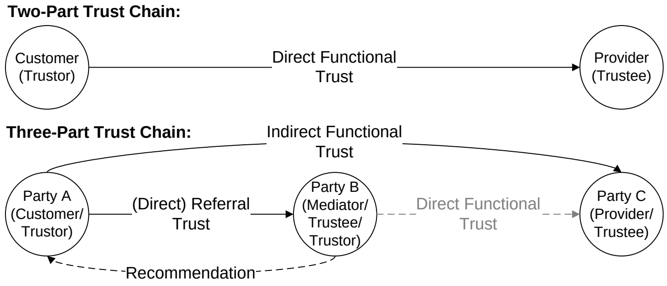


Figure 2. Trust Chains (Jøsang et al., 2006).

In the IS field, several studies discuss trust transitivity and propagation, for example in social media (Qian and Adali, 2014; Basu et al., 2014; Wu et al., 2016; Xiong et al., 2017). However, a sizeable amount of these studies refers to trust as being transitive, which confirms the claim of Sherchan et al. (2013) that the "propagative nature of trust is sometimes confused with the transitive nature of trust". In cloud computing, the concepts of trust transitivity and propagation are rather unexplored. Some articles deal with trust aspects in the context of cooperation with cloud providers or the use of CCS, but in most of the works the emphasis is on direct trust between two actors. Walterbusch et al. (2013), for example, investigate customer trust in mediators and providers. Further, Noor et al. (2013) investigate trust among CCS users and distinguish between explicit as well as transitive user recommendations within a system. Krautheim et al. (2010) propose a cloud trust model based on transitive trust, whereas Singh and Chand (2014) or Pearson (2013) suppose that trust in cloud environments is not transitive.

3 Hypotheses Development

3.1 Functional and Referral Trust

Jøsang and Pope (2005) suggest that the trust of a party *A* (customer) in an indirectly known party *C* (provider) can be influenced to a certain degree by the trust in a directly known party *B* (mediator), which again directly knows party *C*. Trust may change over time (Jøsang and Pope, 2005), especially through events that affect the parties involved or the underlying context (Walterbusch et al., 2013). Not only actions of trustees can impact trust relationships, also incidents occurring independently of the parties involved have to be considered (Jøsang and Pope, 2005). In CC, apart from incidents that have a direct impact on the customer, also perceived events (e.g., a press report) can unfold their influence (Walterbusch et al., 2013). Jøsang and Pope (2005) further argue that trust is weakened by transitivity. Following this, there is no full transitivity of trust in a mathematical, but in a propagative sense (Sherchan et al., 2013). Thus, the trust of party *A* in party *C* is weaker in case party *B* acts as an intermediary between the two parties than in a direct trust relationship between *A* and *C* (Jøsang and Pope, 2005). In case a mediator is interposed, the direct contractual relationship of the customer is transferred from the cloud provider to the mediator, which is then based on a referral trust relationship regarding the mediation of a cloud or an underlying basic service. Hence, the former DFT relationship between the customer and the cloud provider becomes an IFT relationship, dependent on trust transitivity and propagation (Jøsang et al., 2006; Jøsang and Pope, 2005). Therefore, the expansion of a trust chain by additional actors can also have an adverse effect on trust (Jøsang and Pope, 2005). The question arises as to how the FT in a trustee changes when both aspects apply: an event with negative consequences as well as trust transitivity or propagation. In case party *C* is the perpetrator of an event that has negative consequences for party *A*, it is presumed that the respective trust relationship suffers. Also, despite being innocent, a partial liability can be projected to party *B*. This can be explained by the trust that *A* placed in *B* (RT), which allows for the indirect functional trust in *C*. If party *B* is assigned a partial liability for the event, the accusation against the principal perpetrator, party *C*, weakens.

Transferred to CC, the following scenario is conceivable: A customer utilizes an IaaS provider's CCS. This provider runs his own cloud infrastructure to store data. Due to an incident at the provider, the customer cannot access his data temporarily, which adversely influences his business. As a result, the customer's FT in the provider's capabilities decreases. However, if a customer obtains a CCS via a mediator, whose service is based on the service of a third-party provider, the FT decreases to a lower extent. Instead, the customer's RT in the mediator partially decreases, since the latter 'failed' in selecting a reliable basic service provider. Thus, regarding the presence of a mediator, we hypothesize that the customer transfers a partial liability from the provider to the innocent mediator:

H1: *In case a provider is responsible for an incident, a customer's FT in a provider in an indirect trust relationship is higher than in a direct trust relationship, in which the provider can be held solely responsible for the incident.*

In a three-part trust chain, it is assumed that an incident caused by a provider impacts the IFT in the respective provider more strongly than it would be the case if a mediator was to blame. The same applies to the RT in a mediator: if a mediator is responsible, he bears the main blame. Consequently, a customer's RT in the mediator decreases more strongly compared to an incident caused by a provider.

H2: *A customer's IFT in a provider decreases more strongly when an incident is caused by a provider than by a mediator.*

H3: *A customer's RT in a mediator decreases more strongly when an incident is caused by a mediator than by a provider.*

Although the presence of a mediator weakens the trust relationship between a customer and a provider, it is to be assumed that a high level of RT in a mediator has a positive effect on the IFT in a provider. Since a customer relies on a mediator's abilities to select a provider in the customer's sense, a certain degree of trustworthiness of the selected provider can be derived.

H4: *The higher a customer's RT in a mediator, the higher a customer's IFT in a provider.*

3.2 Intention to Use

As trust implies the willingness to be vulnerable to a trustee and his actions, it is always associated with risks (Mayer et al., 1995). In CC, the customer is exposed to various potential risks. These risks are in particular related to data security aspects like storage location, encryption, availability and reliability of services (Zissis and Lekkas, 2012; Ryan, 2011; Keller and König, 2014). It can be further distinguished between a general risk attitude (risk propensity, risk aversion) as well as the perceived risk of a trustor in a concrete situation (Mayer et al., 1995). The latter ultimately affects the actual assumption of a trustor's risk (Mayer et al., 1995). In view of the theory of reasoned action by Fishbein and Ayzen (1975), the belief in something leads to a corresponding attitude, which again leads to a behavioral intention, finally determining the corresponding behavior (McKnight et al., 2002). As a result, trust permits forecasts on the trustor's intention to use (ITU) a trustee's product or service. In general, ITU describes the intention of a person to (continually) use a system (Davis, 1985; Davis, 1989). In

CC, ITU refers to the intention of the customer to (further) use a mediator or provider and their respective CCS (after an incident) (Adelmeyer et al., 2016; Walter et al., 2014). As trust is an important driver of (post-)adoptive behavior (Tams et al., 2017) and based on the theory of reasoned action (Fishbein and Ayzen, 1975) as well as existing work in the field of CC, a positive impact of trust on the ITU a cloud service is assumed (Adelmeyer et al., 2016; Walter et al., 2014). In the present context, a distinction must be made between the intention to use a provider (ITUP) and the intention to use a mediator (ITUM) as well as the corresponding direct (DFT, RT) and indirect trust (IFT) relationships. Concerning a two-part trust relation between a customer and a provider, we hypothesize:

H5: The higher a customer's DFT in a provider, the higher a customer's ITUP.

When considering a three-part trust relationship between a customer, a mediator and a provider, effects of the IFT on both the ITUP and ITUM can be assumed. Further, effects on the RT of a customer in a mediator are conceivable due to a transfer of the fault in case of a negative event. However, given the direct contractual relationship between customer and mediator and the fact that a customer cannot actively choose the basic service provider of a mediator, the effect on the ITUM will be focused:

H6: The higher a customer's IFT in a provider, the higher a customer's ITUM.

H7: The higher a customer's RT in a mediator, the higher a customer's ITUM.

3.3 Disposition to Trust

According to Mayer et al. (1995) and McKnight et al. (1998), for the trustor, a trustee must be trustworthy in organizational contexts. The trustworthiness of a trustee or the trusting beliefs of a trustor are essentially composed of three characteristics: ability/competency, benevolence and integrity (Mayer et al., 1995; McKnight et al., 1998). Transferred to CC, the trustworthiness is largely determined by the capabilities to operate a CCS (provider) or to select an appropriate basic cloud provider (mediator) in the sense of the customer. In addition, the degree of trust towards a trustee is dependent on the individual's propensity to trust or disposition to trust (DT) (Mayer et al., 1995; McKnight et al., 1998). DT describes a trustor's individual property that determines the likelihood that he trusts a party (Mayer et al., 1995). Further, DT can also be defined as the extent to which a person generally tends to depend on others (McKnight et al., 2002), irrespective of information on a particular party. As DT is dependent on the individual's personality (McKnight et al., 1998), the trust in a concrete party tends to vary in a given context. Since research found DT to be an important factor impacting trust of customer's in both CC mediators and providers (Walterbusch et al., 2013), we hypothesize:

H8a: The higher the DT of a customer, the higher its DFT in a provider.

H8b: The higher the DT of a customer, the higher its IFT in a provider.

H8c: The higher the DT of a customer, the higher its RT in a mediator.

3.4 Research Model

The following research model summarizes the respective concepts and hypotheses (cf. Figure 3).

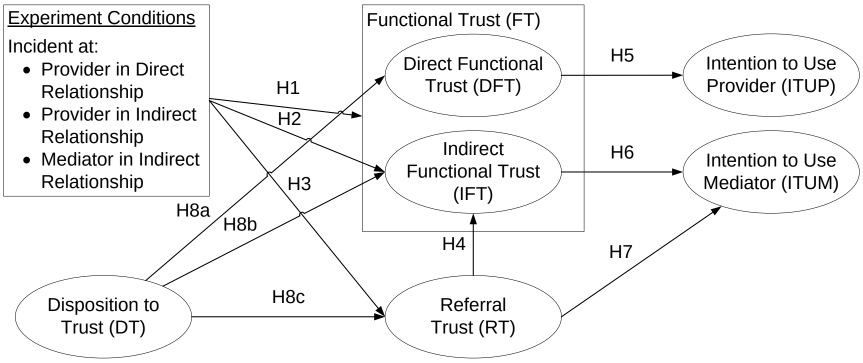

Experiment Conditions
Incident at:
Provider in Direct Relationship
Provider in Indirect Relationship
Mediator in Indirect Relationship
Functional Trust (FT)
Direct Functional Trust (DFT)
Indirect Functional Trust (IFT)
Intention to Use Provider (ITUP)
Intention to Use Mediator (ITUM)
Disposition to Trust (DT)
Referral Trust (RT)
H1
H2
H3
H4
H5
H6
H7
H8a
H8b
H8c

Figure 3. Research Model.

4 Research Method

4.1 Experimental Design and Procedure

Based on the research model, we examine the effects of incidents affecting a mediator and a provider on the respective trust relationships from a customer's point of view by conducting a vignette-based online experiment with manipulations of incidents at the respective actors. In the course of the study, two main aspects are focused: first, the difference between a customer's FT in a provider in a two and a three-part trust chain; second, the effects of incidents at different actors on the respective trust relationships. This requires a closer look at the trust relationship between customer and mediator (RT) and particularly at the mediator's ability to select a suitable basic cloud service provider for its adapted CCS. In these relationships, the participant takes the role of a customer as trustor. To test the hypotheses, three separate participant groups are required. Figure 4 depicts the respective relationships. By means of group 1 (G1) and group 2 (G2), the differences between DFT and IFT in the relationship between customer and provider can be investigated. The customer in G1 is in a direct contractual and trust relationship with the provider. The customer in G2 has a direct contractual relationship with the mediator and, thus, an indirect trust relationship with the provider, who holds the role of the perpetrator of the incident in this test group. Group 3 (G3) is in principle identical to G2 but with the incident taking place at the mediator. In this way the respective effects on the functional or referral trust relationships with varied perpetrators can be investigated. A randomized post-test-only design (Shadish et al., 2002; Recker, 2013) is used as experimental setup. In an unnoticeable first step, the participants are randomly assigned to one of the three experiment groups.

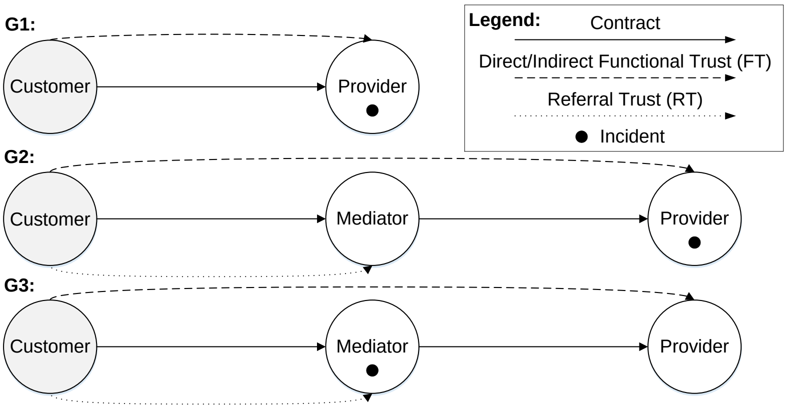
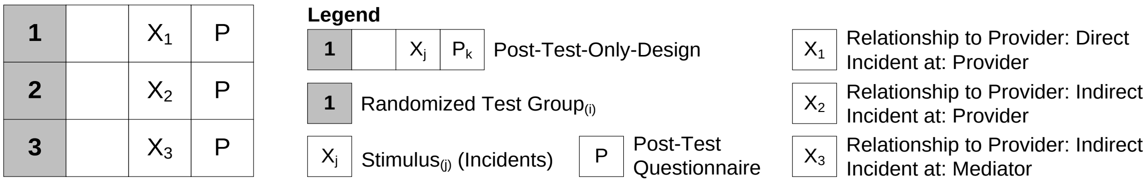


Figure 4. Relationships in the Experimental Groups.

The experiment setup consists of two main components. At first, a vignette is used, which puts the participants into a certain role in a given situation (Finch, 1987; Aguinis and Bradley, 2014). Second, by means of an event (stimulus) the experimental variables are manipulated in order to investigate whether the presumed changes occur. Vignettes can be described as focused descriptions or short stories about hypothetical characters and situations, where the subjects are invited to respond or react in various forms (e.g., decisions, ratings, evaluations etc.) (Finch, 1987; Aronson and Carlsmith, 1968). Our vignette describes the situation of the three main actors - customer, mediator and provider - operating in the cloud ecosystem. The participants are put into the role of an employee working in a fictional company's IT department, a major automotive supplier called *innoTect*, whose future success and continuity depends on a current project. The participants are responsible for the data collected in this project. In the fictive scenario, the project data is outsourced via an IaaS service called *StoreSync* to a mediator (*C-Media*), who in turn utilizes basic cloud services of a third-party cloud provider (*StructureBase*) to store *innoTect*'s data. Within the scenario description, the importance of the data is repeatedly emphasized to maximize the impact on the subjects and their opinions. Thus, in accordance with the work of Mayer et al. (1995), we accent that the outsourcing of the data to the cloud contains risks and that a corresponding incident would have severe consequences. After an event, a serious loss of company data at either the provider (G1 & G2) or the mediator (G3), the participants are asked to provide a supervisor with their personal assessment and opinion of the cloud service. Regarding the different groups and objects of investigation, we made some deviations within the vignette and the post-test by supplementing or removing respective information. Since no mediator exists in G1, the corresponding actor and related information were omitted. The vignette is structured in modules to ensure comparability of the groups. The data is collected in a subsequent survey, in which the subjects are questioned indirectly on the hypothetical constructs by using items (cf. Figure 5).[1]



1		X_1	P
2		X_2	P
3		X_3	P

Legend

1 | | X_j | P_k Post-Test-Only-Design
1 Randomized Test Group$_{(i)}$
X_j Stimulus$_{(j)}$ (Incidents)
P Post-Test Questionnaire
X_1 Relationship to Provider: Direct Incident at: Provider
X_2 Relationship to Provider: Indirect Incident at: Provider
X_3 Relationship to Provider: Indirect Incident at: Mediator

Figure 5. Experiment Setup (Randomized Post-Test-Only-Design).

4.2 Operationalization of Experiment Conditions

In order to operationalize the experiment conditions and the manipulations, we implemented an online-based questionnaire with several consecutive pages, containing textual scenarios that were presented to the participants. Within the scenario description, the first experimental variable is manipulated through the exchangeable contract relation (with mediator in G2 & G3 or without mediator in G1). Following the scenario description, the subjects are confronted with an event (Adelmeyer et al., 2016; Walterbusch et al., 2013). The event, a fire on the provider's (G1 & G2) or the mediator's (G3) premises, results in a serious and irreversible loss of the customer's company data. Since between the respective groups only one variable is altered (ceteris paribus condition), the effects can be assigned to the constructs of the correspondingly manipulated experimental variables (Shadish et al., 2002). To contribute to a better understanding, depictions of the situations (cf. Figure 6) were presented.

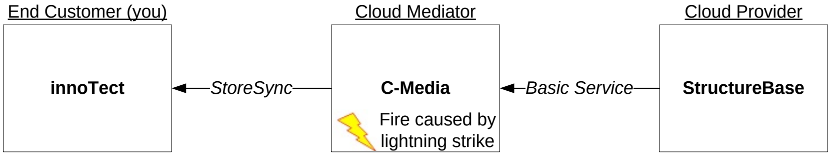


Figure 6. Exemplary Situation Depiction (Stimulus) for G3.

4.3 Operationalization of the Constructs

Since the previously determined hypothetical constructs are not directly measurable, we reviewed theoretical literature to determine appropriate measurement items (questions), which indirectly describe the constructs. FT (DFT and IFT) and RT are described by five items each, one by Bhattacherjee (2002) and four by McKnight et al. (2002). The selection and adaptation of these items is based on the definition of the trust constructs (cf. Table 1), following Jøsang and Pope (2005) and Jøsang et al. (2006). Accordingly, the focus of FT and RT is put on the trustees' abilities in their respective areas (the operation of a CC infrastructure or the selection of IaaS vendors in the sense of the customer). Thus, the measurement of these constructs is exclusively based on questions concerning the trustee's abilities, which allow trust to become transitive (Jøsang et al., 2006). ITUP and ITUM are described by three items by Nicolaou and McKnight (2006), DT is described by respective items by Gefen

[1] The vignette, the constructs, the corresponding items as well as the data collected will be provided to readers interested.

(2000). Because of its ability to measure the general tendency of a person, DT is also suitable as a control variable within the data analysis. Depending on the assignment to the respective groups, the items of the constructs FT (direct and indirect), RT as well as ITUP and ITUM only differ in addressing either the mediator or the provider. The classification of the responses is based on a seven point Likert scale (Likert, 1932) with symmetrically formulated expressions.

Construct	Adapted Definition	Item Source
Direct Functional Trust (DFT)	Trust in the ability of a directly known party in a particular field to perform a particular action which is important to the trustor (Jøsang and Pope, 2005; Jøsang et al., 2006; Mayer et al., 1995). In the context of trust between customers and cloud providers DFT describes the customer's trust in the ability of an IaaS provider, who is the direct contractual partner of the customer, regarding the operation of a CC infrastructure for data storage.	McKnight et al. (2002), Bhattacherjee (2002)
Indirect Functional Trust (IFT)	Trust in the ability of an indirectly known third party in a particular field to perform a particular action which is important to the trustor (Jøsang and Pope, 2005; Jøsang et al., 2006; Mayer et al., 1995). In the context of trust between customers and cloud providers IFT describes the customer's trust in the ability of an indirectly known third-party IaaS provider, from whose basic cloud service the customer is indirectly dependent via the CCS of a mediator as the direct contractual partner of the customer.	McKnight et al. (2002), Bhattacherjee (2002)
Referral Trust (RT)	Trust in the ability of a (directly known) party to refer to or make a recommendation for an indirectly known third party in the trustor's sense (Jøsang and Pope, 2005; Jøsang et al., 2006). In a trust relationship RT "is precisely what allows trust to become transitive" (Jøsang and Pope, 2005). In the present context, RT describes the trust in the ability of the mediator to select a suitable IaaS provider for the adapted CCS in the sense of the customer.	McKnight et al. (2002), Bhattacherjee (2002)
Disposition to Trust (DT)	The individual tendency of a person to trust others or rely on others. Consisting of the belief in the humanity of others as well as the trusting attitude towards others (Mayer et al., 1995; McKnight et al., 1998).	Gefen (2000)
Intention to use a Provider (ITUP)	The behavioral intention of a person to use something (e.g., systems) (Davis, 1989; Nicolaou and McKnight, 2006). In the present context, ITUP describes the intention of a customer to further use a provider in the future for the purposes of data storage or to use his CCS.	Nicolaou and McKnight (2006)
Intention to use a Mediator (ITUM)	The behavioral intention of a person to use something (e.g., systems) (Davis, 1989; Nicolaou and McKnight, 2006). In the present context, ITUM describes the intention of a customer to further use a mediator in the future for the purposes of data storage or to use his CCS.	Nicolaou and McKnight (2006)

Table 1. Constructs and Item Sources.

4.4 Data Collection

The experimental concept was implemented as a web-based questionnaire. In total, 298 undergraduate economics and information systems students were surveyed. Using students as study subjects had the advantage of obtaining a sufficiently large and homogenous sample group, i.e., with regard to age and IS experience (Adelmeyer et al., 2016; Walter et al., 2014). The voluntary participation was rewarded with minor incentives, which were raffled amongst the participants. In the post-test, the items were presented to test the proposed hypotheses and causal relationships of the subsequent constructs (cf. Figure 3). For the analysis, we only considered the 284 completed questionnaires. Besides, aiming at high-quality data, we checked for response patterns and significantly lower overall dwell times (25% faster than average) when conducting the experiment, which led to the omission of seven data sets. In total, 277 questionnaires remained, evenly distributed across the groups (G1 n = 93, G2 n = 92, G3 n = 92) with 65.34% male and 34.66% female participants and an average age of 20.5 years.

5 Data Analysis and Results

5.1 Construct Validity and Reliability

In a first step, we assessed the validity and reliability of the constructs. In order to ensure that the participants were distributed homogeneously among the groups, we conducted *analysis of variance tests* (ANOVA), *Levene tests of variance equality* and *t-tests* for the control variables age, gender, cloud computing experience and disposition to trust (Burns and Burns, 2008). The group-wise comparison of the results indicated no significant differences. Further, we checked for a common method bias (CMB) using Harman's one-factor test (Podsakoff and Organ, 1986). All relevant 17 indicators were examined in a factor analysis, resulting in the extraction of one factor explaining 42.759 percent of the variance. Since the explained variance is below the threshold of 50 percent, a CMB is unlikely (Podsakoff and Organ, 1986; Cenfetelli et al., 2008). To assess one-dimensionality (the extent to which the items measure one construct), we conducted an exploratory factor analysis (EFA). First, we performed an EFA per construct. For the examination the constructs FT (consisting of DFT and IFT) and ITU (consisting of ITUP and ITUM) were aggregated, since the inherent sub-constructs are represented by basically identical items. For all indicators, the determined thresholds for *Measure of Sampling Adequacy* (MSA), *communalities*, the *Kaiser-Meyer-Olkin-criterion* (KMO) and the *Bartlett-test* were met (MSA > .5; communality > .5; KMO > .6 and Bartlett-test < .05) (Burns and Burns, 2008) with the exception of item DT2 (communality .369). Since the communality of FT5 is slightly lower (.556) and FT5 consists of the sub-items IFT5 (.488) and DFT5 (.610) with both having the lowest communality within their item groups and IFT not meeting the threshold, we dropped the corresponding items from further analyses. Using reflective measurements, dropping an item does not affect the meaning of a construct (Jarvis et al., 2003; Burns and Burns, 2008). In addition to the separate EFAs for the different item groups, we conducted a simultaneous EFA for all 17 items (four aggregated constructs DT, FT, RT and ITU) to confirm their assignment to the corresponding constructs. According to Kaiser's rule, we extracted four common factors with an eigenvalue > 1, explaining 71.047% of the overall variance, which confirms our four predetermined aggregated constructs (Burns and Burns, 2008). With factor loadings between .738 and .952 the results are adequate (Hair et al., 1998). Further, the results for KMO (.888), Bartlett-test (.000), MSA (> .731) as well as communalities (> .574) are fully sufficient. In consequence, after dropping items DT2, IFT5 and DFT5, one-dimensionality can be assumed.

Construct	**Items**	**CISC Range**	**N**	**IIC**	**CA**	**CR**	**AVE**	**DT**	**DFT**	**IFT**	**RT**	**ITUP**	**ITUM**
DT	3	.690 - .764	277	.660	.851	.906	.764	.874					
DFT	4	.795 - .858	93	.761	.927	.948	.821	.105	.906				
IFT	4	.731 - .823	184	.681	.891	.927	.761	.015	-	.872			
RT	5	.693 - .809	184	.669	.909	.933	.736	.073	-	.608	.858		
ITUP	3	.926 - .934	93	.907	.966	.978	.938	.125	.875	-	-	.968	
ITUM	3	.882 - .928	184	.884	.958	.973	.923	.086	-	.353	.693	-	.961

The Items DT2, DFT5 and IFT5 were dropped during the EFA; shaded cells: square root of AVE

Table 2. Constructs Attributes.

Subsequently, to assess the construct's internal consistency reliability, we calculated *Cronbach's Alpha* (CA), the *inter-item correlation* (IIC) and the *corrected inter-scale correlation* (CISC) (cf. Table 2). Regarding CA, all constructs meet the recommended threshold value of .7 and can therefore be considered as reliable (Nunnally and Bernstein, 1994). Further, with the majority of the values ranging > .9, the results can be interpreted as highly acceptable (Rossiter, 2002; Burns and Burns, 2008). For IIC, values of > .3 are considered as adequate (Robinson et al., 1991). Regarding CISC, the threshold of .5 is met throughout all items (Zaichkowsky, 1985; Shimp and Sharma, 1987). Further, we assessed the reliability of the constructs in terms of quality criteria of second order by measuring the *indicator reliability* (IR), the *composite reliability* (CR) as well as the *average variances extracted* (AVE). At the indicator level, the required minimum threshold of .4 for IR is widely exceeded by all indicators (> .659). Further, CR and AVE are clearly above the required target values of .6 and .5 for all constructs (Fornell and Larcker, 1981; Bagozzi and Yi, 1988) (cf. Table 2). Thus, the requirements for convergent validity in the context of the construct validity are fulfilled. Further, we evaluated the discriminant validity, which can be assumed when the square roots of the AVE (shaded cells) are higher than the correlations between the constructs (Fornell and Larcker, 1981). Due to the already mentioned systematically missing values, some correlations cannot be calculated (marked with "-" in Table 2). The values of the diagonals are consistently larger than the correlations below, however, the correlation between ITUP and DFT is relatively high (.875). Nevertheless, since the Fornell-Larcker criterion (Fornell and Larcker, 1981) is met and the constructs and underlying items have already been successfully applied together in similar contexts (Adelmeyer et al., 2016; Walter et al., 2014), discriminant validity for all factors is assumed. Thus, the constructs serve as a basis for hypothesis testing.

5.2 ANOVA, Levene's Test and t-Tests Results

To assess the impact of the experimental conditions on the trust constructs, we conducted both analyses of variances (ANOVA and Levene's test) and analyses of means (two-sample t-test). The results revealed a significant difference between G1 & G2 as well as G1 & G3 concerning FT, both regarding variance and mean tests (cf. Table 3). Hence, hypothesis H1 can be confirmed. Between G2 & G3 neither a significant difference of the variances nor mean values of the samples can be confirmed (neither $p < .05$ nor $p < .1$) regarding FT and RT. Thus, hypotheses H2 and H3 are not supported. The reason for this is presumed in the compensating effect of the mediator, to whom a part of the guilt is assigned. This compensation supposedly leads to adjusted trust levels and, thus, aggravates a statistical proof.

Comparison Groups	**Functional Trust (FT)**			**Referral Trust (RT)**		
	Sig. Levene's test	Sig. ANOVA	Sig. t-test	Sig. Levene's test	Sig. ANOVA	Sig. t-test
G1 & G2	.008	.002	.002	-	-	-
G1 & G3	.001	.000	.000	-	-	-
G2 & G3	.699	.243	.243	.812	.289	.289

Table 3. Significance of Levene's Tests, t-Tests and ANOVA for FT and RT.

5.3 Partial Least Squares Analysis

The evaluation of the interdependencies between the constructs and their outcome on the dependent variables and eventually on the remaining hypotheses was conducted using partial least squares structural equation modeling with SmartPLS 3 (Ringle et al., 2012; Ringle et al., 2015; Lowry and Gaskin, 2014). First, we analyzed the model fit. Due to the experimental conditions, the collected data sets partly have missing values (RT is not collected in G1, FT splits into the sub-constructs DFT in G1 and IFT in G2 & G3, ITU is correspondingly divided into ITUP and ITUM). Since complete data are required for the analysis of the model fit, the model is split into two separately considered sub-models (SM). In SM1 the common constructs and data of G1 & G2 are considered, whereas SM2 reflects the data of G2 & G3. The RMSEA values for SM1 (.000) and SM2 (.073) are good or reasonable (Browne and Cudeck, 1993). Further, the requirement for CMIN/DF (CMIN/DF ≤ 2.5) is met (SM1: .985; SM2: 1.988) (Baumgartner and Homburg, 1996). With only marginal restrictions, the SM meet the recommended thresholds (GFI & AGFI $\geq .9$) for GFI (SM1: .967; SM2: .901) and AGFI (SM1: .944; SM2: .861). Since the statistics for SRMR (SM1: .034; SM2: .056) are in line with the recommendations (SRMR $\leq .1$) (Ward et al., 2009), we assume a good model fit.

In a second step, we evaluated the path correlations and coefficients of determination (R^2) of our structural equation model (cf. Figure 7). Since values for path correlations of > .2 indicate significant connections (Chin, 1998a), significant relationships between DFT and ITUP, RT and ITUM as well as RT and IFT can be confirmed. Regarding R^2, values of $\approx .33$ represent a moderate, values of $\approx .67$ a substantial explanation of a construct (Chin, 1998b). Hence, DT neither has a significant impact on DFT nor on RT. However, IFT, ITUP and ITUM can be explained to a large extent by the constructs assigned. Based on the results, a positive influence of DFT on the ITUP in a two-part trust chain and, thus, H5 can be confirmed. Further, H7, according to which a customer's RT in a mediator has a strengthening effect on the ITUM in a three-part trust chain, can be verified. However, since no positive influence of IFT on the ITUM could be proven, H6 is not supported. Furthermore, the model reveals a significant correlation between the RT in a mediator and the IFT in a provider. Since the IFT is to a moderate extent explained by the RT, hypothesis H4 can be confirmed. Thus, the propagation of trust from a mediator to a provider is demonstrated.

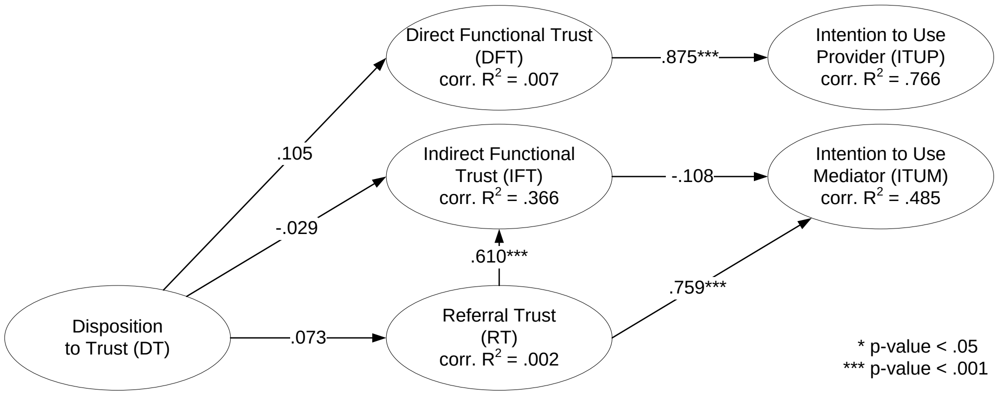


Figure 7. PLS Model.

6 Conclusion

6.1 General Discussion

Based on the results, it is shown that a customer's FT in a cloud provider (after an incident caused by the provider) is higher in an indirect relationship via a mediator than in a direct trust relationship (H1). The reason for this is presumed in the guilt-compensating effect of the intermediary actor, i.e., the assignment of liability to the contractually bound mediator. Thus, the mediator, who has selected the provider on trust of the customer, is given a partial share of the blame for the incident. This compensation is also presumed to account for the non-significant results regarding a customer's FT in a provider or the RT in a mediator after incidents either caused by the mediator or the provider (H2 & H3). However, a strong effect of the RT on the IFT (H4), as well as on the ITUM (H7) and the DFT on the ITUP (H5) could be demonstrated. Thus, in the long term, customers are using providers and mediators whom they trust and concurrent with the trust in the mediator (RT), the trust in the connected provider (FT) increases. Consequently, the propagation of trust in cloud ecosystems and its relevance for cloud adoption and use was demonstrated. Further, the relationship between the trust in a provider and the further use of a mediator (H6) is not significant. We assume that, irrespective of who is to blame for an incident, a customer always assigns the main share of the blame on his direct contract partner (mediator). Significant relationships between the DT on the trust constructs (H8a, H8b and H8c) could also not be verified. We suppose that the reason for this lies in the specially adapted trust constructs and the associated items that describe trust in the specific context of CC, whereas DT reflects a person's general attitude. Table 4 summarizes the status of our hypotheses.

Hypothesis	Relation			Status	Hypothesis	Relation			Status
H1	DFT (G1)	<	IFT (G2)	Supported	H6	IFT ↑	⇒	ITUM ↑	Not Supported
H2	IFT (G2)	<	IFT (G3)	Not Supported	H7	RT ↑	⇒	ITUM ↑	Supported
H3	RT (G2)	>	RT (G3)	Not Supported	H8a	DT ↑	⇒	IFT ↑	Not Supported
H4	RT ↑	⇒	IFT ↑	Supported	H8b	DT ↑	⇒	DFT ↑	
H5	DFT ↑	⇒	ITUP ↑	Supported	H8c	DT ↑	⇒	RT ↑	

Table 4. Overview of Hypotheses.

Regarding the RQs formulated, our experiment revealed that trust in mediators is affected by incidents, irrespective of the liability (RQ2). In this context, the trust in a provider (IFT) is dependent on the interposition of and the corresponding level of RT in a mediator (H1 & H4). In case an incident is caused by a provider, a partial liability is transferred to the mediator, which can be inferred from a lower RT. Trust transitivity in the mathematical sense (full propagation of trust) could not be demonstrated, but a certain level of trust is propagated between the actors in cloud ecosystems (RQ1).

6.2 Implications for Theory and Practice

From a scientific point of view, our findings confirm the importance of trust as a significant factor for the adoption and use of CCS. Our study complements existing literature on trust in CC by expanding two-part trust relationships between customers and providers or the technology itself to three-part relationships between interlinked entities, that are either trusted on a direct or indirect and functional or referral level (Jøsang et al., 2006; Jøsang and Pope, 2005). In this context, we reveal that it is of importance for a customer's trust whether a service is provided directly or indirectly. This is especially relevant since CCS are often based on adapted services of different providers (Floerecke and Lehner, 2016). Thus, the RT in mediators as direct contract partners of customers is of crucial significance.

The proof that trust in a provider depends on the trust in an interposed mediator, including the already discussed mitigating effect on guilt in case of an incident, shows that the adoption and use of CCS via mediators can be advantageous for providers. Hence, service providers could mitigate direct trust issues by providing their services indirectly. Mediators, on the contrary, should be aware of their dependency on providers and the fact that they, as the customer's direct contract partner, can be blamed for (any) incident. Since the IFT plays no significant role regarding the ITUM (lacking support of H6), mediators have also to bear in mind that their relationship with customers largely depends on the level of (referral) trust that a customer puts in the mediator, rather than in the indirectly involved provider. Thus, the careful selection of reliable providers is of high importance. Mediators are further recommended to regularly assure security measures taken by providers, e.g., by demanding certifications for their CCS (Sunyaev and Schneider, 2013). In summary, the creation of a trustworthy business relation and a careful selection of reliable providers are crucial for customer acquisition and loyalty.

6.3 Limitations and Future Research

Like any research endeavor, our study must be viewed in the light of limitations. Since the experiment was based on a fictitious environment using a vignette, it is to be assumed that the participants did not behave as they would in a real environment, e.g. in case they actually have been impacted by a data loss in the cloud (Greenberg and Eskew, 1993; Aguinis and Bradley, 2014). Further, the generalizability of experiments carried out with student participants is discussed controversially in IS (Compeau et al., 2012). However, since the technology usage decisions of students do not differ significantly (Sen et al., 2006; McKnight et al., 2011) and they are deemed early adopters of technological innovations (Gallagher et al., 2001) like cloud computing, we believe that students constitute an adequate target sample for our experiment (Adelmeyer et al., 2016; Walter et al., 2014; Compeau et al., 2012; Gallagher et al., 2001). In addition, as our study targeted the view of individual customers, the generalizability of the results for organizational entities is limited. Since the experiment was carried out online, the results underlie the limitations of web-based experimenting (Reips, 2002). In addition, the structural equation analysis provides best estimation results given a complete data set. However, due to the experimental design and the simultaneous consideration of all constructs, this was not completely fulfilled in our case since the RT could not be collected in G1. In addition, data on the ITUP was collected in G1, while the ITUM was focused in groups G2 & G3. This partly limits the comparability.

In CC, future work on the subject of guilt and trust allocation is promising. For example, further hypothetical constructs (e.g., perceived guilt) as trust influencing factors can be investigated. Similarly, as we purposely used a narrow conceptualization of trust in order to examine the general existence of trust transitivity or propagation, intermediate states and levels of trust, such as trust in the IT artifact or the cloud ecosystem itself (Lansing and Sunyaev, 2016), can be considered. Since the focus of the experiment was put on the intention to use the mediator, it is reasonable to further explore the impact of events on the provider. In addition, the non-significant results regarding the impact of an incident on the trust between customer and provider as well as mediator (H2 and H3) allow for further investigation. For example, events caused more directly by negligence of an actor, such as data breaches, might result in different blame allocations and, thus, in a different manipulation of trust and outcomes of hypotheses. Regarding the results of the vignette study, a practical validation with data from commercial cloud service providers, mediators and their customers as well as actual data losses is desirable.

References

Adelmeyer, M. et al. (2016). "Does the Augmentation of Service Level Agreements affect User Decisions in Cloud Adoption Scenarios? - An experimental Approach." In *Proceedings of the 24th European Conference on Information Systems (ECIS 2016)*. Istanbul: Turkey.

Aguinis, H. and Bradley, K. J. (2014). "Best Practice Recommendations for Designing and Implementing Experimental Vignette Methodology Studies." *Organizational Research Methods* 17(4), pp. 351–371.

Armbrust, M. et al. (2010). "A View of Cloud Computing." *Communications of the ACM* 53(4), pp. 50–58.

Aronson, E. and Carlsmith J. M. (1968). "Experimentation in Social Psychology." In *Handbook of Social Psychology*. Reading, MA, USA: Addison Wesley, pp. 1–79.

Bagozzi, R. P. and Yi, Y. (1988). "On the Evaluation of Structural Equation Models." *Journal of the Academy of Marketing Science* 16(1), pp. 74–94.

Basu, A. et al. (2014). "Opinions of People: Factoring in Privacy and Trust." *ACM SIGAPP Applied Computing Review* 14(3), pp. 7–21.

Baumgartner, H. and Homburg, C. (1996). "Applications of Structural Equation Modeling in Marketing and Consumer Research: A review." *International Journal of Research in Marketing* 13(2), pp. 139–161.

Bhattacherjee, A. (2002). "Individual Trust in Online Firms: Scale Development and Initial Test." *Journal of Management Information Systems* 19(1), pp. 211–242.

Böhm, M. et al. (2010). "Towards a Generic Value Network for Cloud Computing." In *Proceedings of the 7th International Workshop on Economics of Grids, Clouds, Systems, and Services*. Ischia: Italy, pp. 129–140.

Browne, M. and Cudeck, R. (1993). "Alternative Ways of Assessing Equation Model Fit." In *Testing Structural Equation Models*. Ed. by K. A. Bollen and J. S. Long. Newbury Park: Sage, pp. 136–162.

Burns, R. B. and Burns, R. A. (2008). *Business Research Methods and Statistics Using SPSS*, London, Thousand Oaks, CA, New Delhi, Singapore: Sage.

Cenfetelli, R. T., Benbasat, I. and Al-Natour, S. (2008). "Addressing the What and How of Online Services: Positioning Supporting-Services Functionality and Service Quality for Business-to-Consumer Success." *Information Systems Research* 19(2), pp. 161–181.

Chin, W. W. (1998a). "Issues and Opinion on Structural Equation Modeling Clear Reporting." *MIS Quarterly* 22(1), pp. vii–xvi.

Chin, W. W. (1998b). "The Partial Least Squares Approach for Structural Equation Modeling." In *Modern Methods for Business Research*. Ed. by G. A. Marcoulides. Mahwah, NJ, London: Lawrence Erlbaum Associates Publishers, pp. 295–336.

Christianson, B. and Harbison, W. S. (1996). "Why Isn't Trust Transitive?" In *Security Protocols*. Springer Berlin Heidelberg, pp. 171–176.

Chu, R., Lai, I. K. W. and Lai, D. C. F. (2013). "Trust Factors Influencing the Adoption of Cloud-Based Interorganizational Systems: A Conceptual Model." In *Proceedings of the 2013 International Conference on Engineering, Management Science and Innovation (ICEMSI)*. Taipa: Macao.

Compeau, D. et al. (2012). "Research Commentary: Generalizability of Information Systems Research Using Student Subjects - A Reflection on Our Practices and Recommendations for Future Research." *Information Systems Research* 23(4), pp. 1093–1109.

Davis, F. D. (1985). *A Technology Acceptance Model for Emperically Testing New End-User Information Systems: Theory and Results*. Massachusetts Institute of Technology.

Davis, F. D. (1989). "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology." *MIS Quarterly* 13(3), pp. 319–340.

Drago, I. et al. (2012). "Inside Dropbox: Understanding Personal Cloud Storage Services." *Proceedings of the 2012 ACM Conference on Internet Measurement*. Boston, MA: USA, pp. 481–494.

Finch, J. (1987). “The Vignette Technique in Survey Research.” *Sociology* 21(1), pp. 105–114.

Fishbein, M. and Ayzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, Reading, MA, USA: Addison-Wesley.

Floerecke, S. and Lehner, F. (2016). “Cloud Computing Ecosystem Model: Refinement and Evaluation.” In *Proceedings of the 24th European Conference on Information Systems (ECIS 2016)*. Istanbul: Turkey.

Fornell, C. and Larcker, D. F. (1981). “Evaluating Structural Equation Models with Unobservable Variables and Measurement Error.” *Journal of Marketing Research* 18(1), pp. 39–50.

Gallagher, K., Parsons, J. and Foster, K. (2001). “A Tale of Two Studies: Replicating Advertising Effectiveness and Content Evaluation in Print and on the Web.” *Journal of Advertising Research* 41(4), pp. 71–81.

Garrison, B. G., Kim, S. and Wakefield, R. L. (2012). “Success Factors for Deploying Cloud Computing.” *Communications of the ACM* 55(9), pp. 62–68.

Géczy, P., Izumi, N. and Hasida, K. (2012). “Cloudsourcing: Managing Cloud Adoption.” *Global Journal of Business Research* 6(2), pp. 57–70.

Gefen, D. (2000). “E-Commerce: the Role of Familiarity and Trust.” *Omega* 28(6), pp. 725–737.

Greenberg, J. and Eskew, D. E. (1993). “The Role of Role Playing in Organizational Research.” *Journal of Management* 19(2), pp. 221–241.

Hair, J. F. et al. (1998). *Multivariate Data Analysis*. 5th Edition. Upper Saddle River, NJ: Prentice-Hall International.

Huang, J. and Fox, M. S. (2006). “An Ontology of Trust – Formal Semantics and Transitivity.” In *Proceedings of the 8th International Conference on Electronic Commerce (ICEC)*. Fredericton: Canada, pp. 259–270.

Jarvis, C. B., MacKenzie, S. B. and Podsakoff, P. M. (2003). “A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research.” *Journal of Consumer Research* 30(2), pp. 199–218.

Jøsang, A., Hayward, R. and Pope, S. (2006). “Trust Network Analysis with Subjective Logic.” In *Proceedings of the 29th Australasian Computer Science Conference (ACSC)*. Tasmania: Australia, pp. 85–94.

Jøsang, A. and Pope, S. (2005). “Semantic Constraints for Trust Transitivity.” In: *Proceedings of the 2nd Asia-Pacific Conference on Conceptual Modelling*. Newcastle: Australia, pp. 59–68.

Keller, R. and König, C. (2014). “A Reference Model to Support Risk Identification in Cloud Networks.” In: *Proceedings of the 35th International Conference on Information Systems (ICIS 2014)*. Auckland: New Zealand.

Ko, R. K. L. et al. (2011). “TrustCloud: A Framework for Accountability and Trust in Cloud Computing.” In: *Proceedings of the 2011 IEEE World Congress on Services (SERVICES)*. Washington, DC: USA, pp. 584–588.

Krautheim, F. J., Phatak, D. S. and Sherman, A. T. (2010). “Introducing the Trusted Virtual Environment Module: A new Mechanism for Rooting Trust in Cloud Computing.” In: *Trust and Trustworthy Computing. Trust 2010. Lecture Notes in Computer Science*. pp. 211–227.

Lansing, J. and Sunyaev, A. (2016). “Trust in Cloud Computing: Conceptual Typology and Trust-Building Antecedents.” *ACM SIGMIS Database* 47(2), pp. 58–96.

Leimeister, S. et al. (2010). “The Business Perspective of Cloud Computing: Actors, Roles, and Value Networks.” In: *Proceedings of 18th European Conference on Information Systems ECIS 2010*. Pretoria: South Africa.

Likert, R. (1932). “A Technique for the Measurement of Attitudes.” *Archives of Psychology* 22(140), p. 55.

Lowry, P. B. and Gaskin, J. (2014). “Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose it and How to Use it.” *IEEE Transactions on Professional Communication* 57(2), pp. 123–146.

Marston, S. et al. (2011). “Cloud Computing - The Business Perspective.” *Decision Support Systems* 51(1), pp. 176–189.

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.

McKnight, D. H. et al. (2011). “Trust in a Specific Technology: An Investigation of Its Components and Measures.” *ACM Transactions on Management Information Systems* 2(2).

McKnight, D. H., Choudhury, V. and Kacmar, C. (2002). “Developing and Validating Trust Measures for e-Commerce: An Integrative Typology.” *Information Systems Research* 13(3), pp. 334–359.

McKnight, D. H., Cummings, L. L. and Chervany, N.L. (1998). “Initial Trust Formation in New Organizational Relationships.” *Academy of Management Review* 23(3), pp. 473–490.

Nicolaou, A. I. and McKnight, D. H. (2006). “Perceived Information Quality in Data Exchanges: Effects on Risk, Trust, and Intention to Use.” *Information Systems Research* 17(4), pp. 332–351.

Noor, T. H. et al. (2016). “Managing Trust in the Cloud: State of the Art and Research Challenges.” *Computer* 49(2), pp. 34–45.

Noor, T. H. et al. (2013). “Trust Management of Services in Cloud Environments: Obstacles and Solutions.” *ACM Computing Surveys* 46(1), pp. 1–30.

Nunnally, J. C. and Bernstein, I. H. (1994). *Psychometric Theory*. 3rd Edition. New York: McGraw-Hill.

Pearson, S. (2013). “Privacy, Security and Trust in Cloud Computing.” In *Privacy and Security for Cloud Computing*. Ed. by S. Pearson and G. Yee. London: Springer, pp. 3–42.

Pearson, S. and Benameur, A. (2010). “Privacy, Security and Trust Issues Arising from Cloud Computing.” In *Proceedings of the 2010 IEEE 2nd International Conference on Cloud Computing Technology and Science (CloudCom)*. Indianapolis, IN: USA, pp. 693–702.

Podsakoff, P. M. and Organ, D. W. (1986). “Self-Reports in Organizational Research: Problems and Prospects.” *Journal of Management* 12(4), pp. 531–544.

Qian, Y. and Adali, S. (2014). “Foundations of Trust and Distrust in Networks: Extended Structural Balance Theory.” *ACM Transactions on the Web* 8(3), pp. 1–33.

Recker, J. (2013). *Scientific Research in Information Systems: A Beginner’s Guide*, Heidelberg: Springer.

Reips, U. D. (2002). “Standards for Internet-Based Experimenting.” *Experimental Psychology* 49(4), pp. 243–256.

Ringle, C. M., Sarstedt, M. and Straub, D. W. (2012). “Editor’s Comments - A Critical Look at the Use of PLS-SEM in MIS Quarterly.” *MIS Quarterly* 36(1), pp. iii–xiv.

Ringle, C. M., Wende, S. and Becker, J. M. (2015). *SmartPLS 3*. Available at: http://www.smartpls.com.

Robinson, J. P., Shaver, P. R. and Wrightsman, L. S. (1991). “Criteria for Scale Selection and Evaluation.” *Measures of Personality and Social Psychological Attitudes* 1(3).

Rossiter, J. R. (2002). “The C-OAR-SE Procedure for Scale Development in Marketing.” *International Journal of Research in Marketing* 19(4), pp. 305–335.

Ryan, M. D. (2011). “Cloud Computing Privacy Concerns on Our Doorstep.” *Communications of the ACM* 54(1), pp. 36–38.

Sen, R., King, R. C. and Shaw, M. J. (2006). “Buyers’ Choice of Online Search Strategy and Its Managerial Implications.” *Journal of Management Information Systems* 23(1), pp. 211–238.

Shadish, W. R., Cook, T. D. and Campbell, D. T. (2002). *Experimental and Quasi-Experimental Designs for Generalized Causal Inference*. Boston, New York: Houghton Mifflin Company.

Sherchan, W., Nepal, S. and Paris, C. (2013). “A Survey of Trust in Social Networks.” *ACM Computing Surveys (CSUR)* 45(4), pp. 1–33.

Shimp, T. A. and Sharma, S. (1987). “Consumer Etnocentrism: Construction and Validation of the CETSCALE.” *Journal of Marketing Research* 24(3), pp. 280–289.

Singh, S. and Chand, D. (2014). “Trust Evaluation in Cloud Based on Friends and Third Party’s Recommendations.” In: *Proceedings of the 2014 Recent Advances in Engineering and Computational Sciences (RAECS)*. Chandigarh: India.

Tams, S., Thatcher, J. B. and Craig, K. (2017). “How and Why Trust Matters in Post-Adoptive Usage: The Mediating Roles of Internal and External Self-Efficacy.” *Journal of Strategic Information Systems*, in press, corrected proof.

Walter, N. et al. (2014). "“May I help You?” Increasing Trust in Cloud Computing Providers through Social Presence and the Reduction of Information Overload." In *Proceedings of the 2014 International Conference on Information Systems (ICIS 2014)*. Auckland: New Zealand.

Walterbusch, M., Martens, B. and Teuteberg, F. (2013). "Exploring Trust in Cloud Computing: A Multi-Method Approach." In *Proceedings of the 21st European Conference on Information Systems (ECIS 2013)*. Utrecht: Netherlands.

Ward, C. et al. (2009). "The Convergent, Discriminant, and Incremental Validity of Scores on a Self-Report Measure of Cultural Intelligence." *Educational and Psychological Measurement* 69(1), pp. 85–105.

Wu, J., Xiong, R. and Chiclana, F. (2016). "Uninorm Trust Propagation and Aggregation Methods for Group Decision Making in Social Network With Four Tuple Information." *Knowledge-Based Systems* 96, pp. 29–39.

Xiong, F., Liu, Y. and Cheng, J. (2017). "Modeling and Predicting Opinion Formation With Trust Propagation in Online Social Networks." *Communications in Nonlinear Science and Numerical Simulation* 44, pp. 513–524.

Yu, B. and Singh, M. P. (2000). "A Social Mechanism of Reputation Management in Electronic Communities." In: *Proceedings of the 4th International Workshop on Cooperative Information Agents*. Boston, MA: USA, pp. 154–165.

Zaichkowsky, J. L. (1985). "Measuring the Involvement Construct." *The Journal of Consumer Research* 12(3), pp. 341–352.

Zissis, D. and Lekkas, D. (2012). "Addressing Cloud Computing Security Issues." *Future Generation Computer Systems* 28(3), pp. 583–592.