CORA Cork Open Research Archive
Cartlann Taighde Oscailte Chorcaí

Title	Building consumer trust in the cloud: an experimental analysis of the cloud trust label approach
Authors	van der Werff, Lisa;Fox, Grace;Masevic, Ieva;Emeakaroha, Vincent C.;Morrison, John P.;Lynn, Theo
Publication date	2019-04-24
Original Citation	van der Werff, L., Fox, G., Masevic, I., Emeakaroha, V.C., Morrison, J.P. and Lynn, T., 2019. Building consumer trust in the cloud: an experimental analysis of the cloud trust label approach. Journal of Cloud Computing, 8(1), (6). DOI:10.1186/s13677-019-0129-8
Type of publication	Article (peer-reviewed)
Link to publisher's version	https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-019-0129-8 - 10.1186/s13677-019-0129-8
Rights	© The Author(s). 2019 - https://creativecommons.org/licenses/by/4.0/
Download date	2026-11-04 11:06:18
Item downloaded from	https://hdl.handle.net/10468/9084

UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

van der Werff et al. Journal of Cloud Computing: Advances, Systems and Applications (2019) 8:6
https://doi.org/10.1186/s13677-019-0129-8

Journal of Cloud Computing: Advances, Systems and Applications

RESEARCH Open Access

Building consumer trust in the cloud: an experimental analysis of the cloud trust label approach

Lisa van der Werff[1*], Grace Fox[1], Ieva Masevic[2], Vincent C. Emeakaroha[3], John P. Morrison[4] and Theo Lynn[1]

Abstract

The lack of transparency surrounding cloud service provision makes it difficult for consumers to make knowledge based purchasing decisions. As a result, consumer trust has become a major impediment to cloud computing adoption. Cloud Trust Labels represent a means of communicating relevant service and security information to potential customers on the cloud service provided, thereby facilitating informed decision making. This research investigates the potential of a Cloud Trust Label system to overcome the trust barrier. Specifically, it examines the impact of a Cloud Trust Label on consumer perceptions of a service and cloud service provider trustworthiness and trust in the cloud service and cloud service provider. An experimental study was carried out with a sample of 227 business decision makers with data collected before exposure to the label to examine initial perceptions and after exposure to the label to examine any change in perceptions and attitudes. As hypothesised, the results suggest that Cloud Trust Labels that contain positive information can have a positive impact on trust and trustworthiness while Cloud Trust Labels that contain negative information have a negative impact. The practical implications of this new method of communicating trustworthiness online are discussed and recommendations are made for future research.

Keywords: Cloud computing, Trust, Trustworthiness, cloud trust label, Sensemaking

Introduction

Recent years has seen growing interest and investment in cloud computing, defined by the National Institute of Standards and Technology (NIST) as a model for "enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, application, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1]. Cloud computing provides service offerings at three different levels - Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [2, 3]. Cloud computing offers broad ranging benefits to organisations of all sizes from location independence to scalability and cost effectiveness [3–5]. Growth in the area is forecast to continue with the public cloud services market alone estimated to be worth $383 billion by 2020 and predictions that cloud computing will affect over 50% of Information Technology (IT) outsourcing deals [6].

Despite positive forecasts and its transformative potential, cloud computing remains in the early stages of diffusion with many decision makers hesitant to adopt [7]. One of the core barriers facing adoption and the exploitation of the benefits of the cloud is trust [8]. Trust refers to an individual or organisation's willingness to be vulnerable to another party based on positive expectations of their behaviour [9]. The importance of trust in the cloud computing context has been repeatedly highlighted due to the lack of transparency surrounding cloud offerings [4], and customers' inability to fully audit cloud services [7]. As such, identifying ways to resolve this barrier to adoption has become the focus of policy makers, academic scholars and industry practitioners alike.

As a forum for business transactions, the online environment is characterised by high levels of uncertainty

* Correspondence: lisa.vanderwerff@dcu.ie
[1]Irish Institute of Digital Business, Dublin City University Business School, Dublin, Ireland
Full list of author information is available at the end of the article

Springer Open

© The Author(s). 2019 **Open Access** This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

and risk, making trust vital to enabling cooperation and interaction [10]. In addition, the online environment typically presents an overwhelming amount of complex information and options to consumers who often possess far less understanding of the context and products on offer than the parties who offer these online services. Across online and offline contexts, this level of potential risk, complexity and uncertainty has the potential to significantly hamper exchange efforts [11]. This is particularly true in the early stages of interaction with a new technology [12] and even more so in the early stages of the technology adoption decision making process [13]. Although trust has the capacity to mitigate these issues, high levels of uncertainty and ambiguity have been shown to encourage intuitive and heuristic processing [14, 15], where individuals make snap decisions without rational consideration of available information. In the case of cloud computing, where trust is core to adoption decision making [4] and a general lack of trust prevails [8], consumer reliance on heuristic decision making that is consistent with currently held opinions may be detrimental to cloud providers. From the consumer standpoint, a lack of rational, deliberative decision making may drive suboptimal decisions based on a fear of new technology and reinforce delays in capitalising on the benefits of the cloud.

The challenge for service providers in this relatively new environment is to encourage potential consumers to engage in deliberative and systematic consideration of the attributes of a service before making a trust decision. Traditional methods of communicating trustworthiness are somewhat problematic for the cloud industry and typically provide only high-level information about the product. Indeed, while it is possible for individuals to trust technology and technology providers [16], it is difficult for consumers to trust online services due to the absence of cues that would typically be available in the offline context [17]. As a result, alternative trust building mechanisms have been proposed [18, 19]. These include the development of frameworks and models identifying trustworthy cloud providers [17, 20, 21], reputation, measurement and rating systems [19, 22, 23], service level agreement (SLA)-verification based trust, cloud transparency mechanisms, trust-as-a-service, formal accreditation, standards, audit, and related assurance seals [19, 22].

One recent suggestion has been the use of a trust label to provide consumers with a visual, real time summary of a range of relevant security and service information about a particular cloud service [18, 22]. The trust label builds upon the nutritional privacy label approach developed and validated in prior work as a means of communicating in a transparent manner with consumers [24, 25] and incorporates approaches identified in extant literature including SLA-verification based trust and cloud transparency mechanisms [19, 22, 23, 26]. Drawing on the sensemaking perspective [27], we argue that the Cloud Trust Label (CTL) approach offers cloud service providers (CSPs) or relevant institutional authorities with a means to communicate the attributes of a cloud service transparently with potential consumers impacting perceptions of trustworthiness and trust. In gaining access to this information, consumers can make knowledge based trust decisions where they have actively processed information about the service *and* service provider and have gathered 'good reasons' for their trust perceptions [28].

Our study makes a number of contributions to theory and practice. Firstly, while many scientific publications propose trust mechanisms in a cloud computing context, few empirically validate their claims relating to trust building. This study seeks to experimentally validate the impact of a trust mechanism, in this case positive and negative CTLs, on consumer perceptions of a cloud-based SaaS customer relationship management (CRM) system. As such, this research contributes to academic and practice-oriented literatures on both trust in SaaS deployment models and cloud computing, in general. Leading scholars have issued repeated called for more contextualised trust theory and research [29, 30] and cloud computing represents a complex context, both in terms of adoption decision making and trust. To date, existing literature has examined trust as an antecedent to adoption [31]. This research moves beyond trust as a predictor of cloud adoption to investigate the effectiveness of the CTL approach in signalling trustworthiness to cloud consumers [32]. Secondly, this paper addresses calls for researchers to explore the relationships between trust in IT artefacts and trust in organisations or individuals providing an IT service. In this way, our study contributes to both theory and practice by exploring the inter-relationship between trust in the cloud service and trust in the cloud service provider. Thirdly, the paper makes a very significant practical contribution. The implementation of cloud services has been identified as one of the top three technology management issues faces by companies [33]. This paper validates a new solution for CSPs or institutional authorities in the cloud environment seeking to communicate openly with potential consumers in a way that impacts trust.

The remainder of this article is structured as follows. The next section reviews relevant literature relating to trust decisions in cloud computing selection and summarises various trust mechanisms presented in the literature. We then present two cloud trust labels for cloud computing based on prior work and extant literature and our hypotheses for experimental validation. The study design, sample, and measures used in our experiment are then described. Next the results are presented and

discussed. The paper finishes with an overview of limitations and future avenues for research and some concluding remarks.

Literature review

Unsurprisingly, increased investment in cloud computing has spurned growing interest in the form of academic research. The majority of this research utilises constructs rooted in technology adoption models to explore the predictors of cloud computing adoption across a variety of contexts and cultures. However, there exists little consensus on which technology adoption model best fits the cloud computing context [2]. Furthermore, some studies have explored technological factors without drawing on a guiding framework [34], with others combining validated models with important contextual factors such as risk and trust. These studies have found that trust beliefs positively influence attitudes towards adoption and intention to adopt cloud services among students, teachers and consumer samples [3, 4, 31, 35]. The importance of trust in the cloud computing context is therefore apparent. This is unsurprising given the influence of trust in other contexts on outcomes such as acceptance and use of a new technology [36, 37] and purchasing decisions [38]. Indeed, some scholars claim trust can be considered the most important factor in the exchange of resources online [39]. Despite this growing new body of literature, trust continues to represent a barrier to cloud computing adoption. Thus, this research seeks to understand how trustworthiness can be influenced using trust labels and therefore seeks to provide actionable insights to build trust in the complex and uncertain context of cloud computing.

Trust decisions in cloud service selection

Our conceptualisation of trust in this study is based on Rousseau et al.'s [9] definition of trust as a *psychological state comprising the intention to accept vulnerability based on positive expectations of the intentions or behaviour of another.*

In order to establish trust in interacting with a cloud service, consumers must be willing to accept vulnerability to both the IT artefact and the company providing that technology. As a result, the focus of trust in our research is on trust both in the cloud provider and in the cloud product. In the case of the cloud provider, Rousseau's definition can be applied as it stands. However, in line with McKnight [40], we argue that trust in the cloud product or technology reflects a willingness to be vulnerable in relation to depending on the technology to carry out a task. In either case, this willingness is said to be based on perceptions of trustworthiness of the other party or product. Trustworthiness typically represents an evaluation or judgment of the other party aggregated from perceptions of benevolence, integrity and ability [41]. Benevolence refers to the perception that the other party has your best interests at heart, while integrity perceptions are concerned with the consistency, principles and morals of the other party. Ability refers to the perception that the other party has the competence, knowledge or skills to carry out a particular task. The sub dimensions of trustworthiness have been adapted to apply to trust in technology as reliability, functionality and helpfulness [29].

In an online environment, trust building is often more complex, and the absence of physical cues can make it difficult for organisations to build trust in the early yet crucial stages of a relationship [17]. However, trustworthiness can be built in this context and can be based on individual human constructs such as integrity or system level constructs such as reliability [16]. More specifically, in the cloud computing context, perceptions of trustworthiness may be based on knowledge and online cues including website design, feedback reputation systems, feedback reputation systems, third party assurances, cloud transparency mechanisms and more technical trust mechanisms including so-called SLA-verification, "Trust-as-a-Service" and other methods.

Website design and aesthetics including colours, graphics and layout have been shown to have an important impact on perceptions of trustworthiness in online vendors [42]. Indeed, consumers have been shown to reject websites due to website design issues before ever systematically reviewing the content of the website [43]. Aesthetics and design features appear to act as an important heuristic cue for guiding consumer behaviour. Unfortunately, a universally pleasing visual design is difficult to achieve as aesthetic preferences differ across demographic characteristics such as culture and gender [44, 45]. Overall, these mechanisms for building trust require consumers to make generalisations based on the experience and endorsement of others or on the aesthetic qualities of a vendor's online shopfront. At best, these mechanisms can only encourage a suspicious, calculative form of trust where consumers assess whether the potential benefits outweigh the potential costs in light of systems that may constrain untrustworthy behaviour (e.g. loss of accreditation or negative feedback reviews). In the absence of either personal experience or detailed information about product and provider performance, it is impossible for consumers to make more robust knowledge based trust judgments. Indeed, trust theory suggests that perceptions of behavioural constraints and cost-benefit analyses may be enough to eliminate distrust but not to develop trust or the many benefits that accompany it [46, 47]. Knowledge based trust is less fragile than its calculative alternative [47] and as such provides a stronger foundation for risk taking behaviour and the development of an ongoing relationship between the

consumer and the CSP. As existing methods of building consumer trustworthiness are likely to be unsuccessful in a cloud computing context, cloud providers need to find a way to create positive impressions of their products and encourage consumers to make more personal, knowledge based trust decisions about a product before they have had experience using the system.

The central trust building mechanism in e-commerce to date has been reputation systems [39, 48]. Reputation systems operate at a peer to peer level and offer community-based feedback on consumer perceptions of a product, provider or service. The system is proposed to act as a signal of trustworthiness based on third party previous experience and by providing an incentive for vendors to behave in a trustworthy manner [37]. These systems are typical in large e-commerce marketplaces with large customer bases where consumers and vendors engage in short-term and often one-off transactions [49]. In contrast, many cloud technologies are provided with a view to long-term service provision by companies with a smaller customer base making feedback systems less appropriate. In addition, trustworthiness is subjective [50] and what is most important to one consumer in terms of functionality may not be important to another. In the cloud computing context, Baldwin and colleagues [51] discuss how stakeholders make trade-offs against security considerations including confidentiality, availability, and cost. For example, in the case of CRM systems, continuous availability is a primary concern whereas for batch processing in the cloud, such as 3D image rendering, on-demand scalability, availability of specialist resources (e.g. graphics processing units), confidentiality and cost may be more important. Notwithstanding this, there have been numerous proposals for cloud rating systems however such proposals have yet to garner significant traction in the marketplace [19, 22, 23, 26, 52].

An alternative form of third party endorsement is that of an assurance seal or trust mark displayed through a logo or seal on the vendor's website. This seal acts as a visual cue or signal of credibility through endorsement by an independent third party [53]. Assurance seals are proposed to work through a process of transference of trust [54] from the independent third party to the online vendor in question. However, research has demonstrated increasingly mixed findings about the impact of such seals with some scholars reporting that the majority of online consumers place little or no weight on their presence [55]. McKnight and colleagues [56] propose that instances where assurance seals are noticed but not considered in making the trust decision may be due to a lack of understanding of what the seal signals and a failure of seals to provide specific information about security issues.

A number of technical solutions to addressing trust issues in cloud computing have been proposed although there is little evidence of validation that these mechanisms do build trust or mitigate and repair distrust. Numerous authors seek mechanisms to verify that CSPs are meeting their quality of service (QoS) levels as defined in the SLA between the CSP and the client. So-called SLA-verification based methods seek to build trust through QoS monitoring of SLAs [19, 22, 57]. Such mechanisms are often provided to some degree by CSPs through on-demand cloud transparency mechanisms that provide information on "elements of transparency" which may include service performance, security etc. [19, 58, 59]. Similarly, other cloud transparency mechanisms seek to bridge the gap between transparency and assurance seals through publicly accessible self-assessments of internal controls [19, 22]. One such initiative by the Cloud Security Alliance (CSA), the Security, Trust & Assurance (STAR) Registry has gained some traction and is widely cited [59]. Numerous attempts have been made to establish more "formal" trust mechanisms. RSA and ZScaler launched a single-point service for configuring and managing security of cloud services from multiple CSPs [60]. Huang et al. (2013) have proposed a trust model based on "formal" certification and chains of trust for validation of attributes of a cloud service or its provider. More recently, the emergence of blockchain has resulted in numerous proposals relating to its use to secure the cloud [61]. Notwithstanding numerous proposals for technology-based solutions to trust issues, there is little validation in the literature that such proposals build trust with target end users Table 1.

The process through which individuals strive to understand issues that are novel, ambiguous or confusing is generally known in the organisational literature as sensemaking [27, 62]. The emerging nature of the cloud industry means that consumer purchasing decisions in the cloud environment have the potential to possess all of these characteristics. From a sensemaking perspective, individuals' perceptions of another party can be seen to unfold over time as a process which is influenced by interpretation of information presented in the environment. Garrison and colleagues [63] note that trust in cloud computing develops through communication, procurement, and transactional activities, culminating in the IT manager's perception that the vendor is trustworthy, reliable, even-handed, and working in the best interests of the client. Making sense of risk in a cloud computing context depends on both experience with the vendor and the transparency (or opacity) of the actual cloud service and the assurance information on cloud service levels available at any given time for a given period [51]. However, as an effortful process, sensemaking does not happen continuously over time and Weick and Sutcliffe [64] describe a triggering process whereby sensemaking is portrayed as a disruption in current understanding caused by unexpected information which is deemed

Table 1 Summary of Trust Mechanisms Impacting Cloud Computing

Trust Mechanisms	Example	References
Website design	The design, colours and aesthetics impact the perceptions of trustworthiness of online vendors.	[42, 44, 45]
Feedback Reputation systems	Comprehensive score reflecting an overall opinion or an aggregate of scores on several major aspects of performance.	[19, 22, 23, 26, 52, 84]
Third Party Assurances	Third party attestation, certification and/or assurances seals e.g. ISO/IEC 27001.	[19, 22, 85]
Cloud transparency mechanism	• Publicly accessible self-assessment of security controls e.g. Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR).	[19, 22, 59]
	• On-demand access to information on "elements of transparency" e.g. CSA CloudTrust Protocol.	[19, 58, 59]
SLA-verification based trust	Quality of service monitoring based on pre-defined SLA service levels.	[19, 22, 23, 57]
Trust as a Service	Single point service for configuring and managing security of cloud services from multiple service providers.	[19, 60]
"Formal" trust mechanisms	Trust based on "formal" certification and chains of trust for validation of attributes of a cloud service or its provider.	[19, 61]
Trust Label	Standardised label that presents a visual, real time summary of a range of relevant security and service information about a particular cloud to consumers in an easily understandable format.	[16, 58, 73, 86]

important enough to motivate more mindful consideration of the issue. Cognitive science suggests that effortful consideration of information is engaged only when more automatic processes encounter unexpected information [65]. However, when the trusting individual has a strong existing perception of the other party, whether positive or negative, confirmation biases can make automatic processes less sensitive to discrepancy [66]. As a result, subtle cues of trustworthiness where trust is inferred through association with others or through small trustmarks appearing on websites may not be enough to motivate a shift to effortful decision making.

Sensemaking is a social process involving the actions and interpretations of more than one party. Indeed, through the process of sensegiving, individuals and organisations can influence the sensemaking process of other parties [67]. Moreover, in situations where individuals have already engaged in sensemaking and established a particular point of view, sensebreaking can be used to motivate them to reconsider their position and re-evaluate their actions [62, 68]. Sensebreaking involves questioning and reframing previous conceptions and can be achieved through the presentation of contradictory information [69] and creates a "meaning void" that individuals will then seek to fill [70]. Processes of sensemaking, sensebreaking and sensegiving can then be seen to take place in an iterative cycle [67].

Proposed model In order to build trust in cloud services we argue that stakeholders in the cloud industry (CSPs, institutional authorities or both) need to engage in this process with consumers providing enough information about cloud products to break any existing fears or stereotypes about the Cloud and give sense to their decisions about which services and service provider to trust. A method which might allow stakeholders to engage in this process is a CTL proposed by [18]. The label is based on the nutritional food label and recent literature in the privacy domain [24, 25] which developed privacy labels to communicate privacy practices with consumers and has been extended to influence privacy perceptions in Brazilian and Irish contexts [71, 72]. The information included in the label was decided through a Delphi process which involved a range of stakeholders from the Cloud computing industry drawing on factors influencing trust in the cloud as highlighted in prior literature [18, 73, 74]. The proposed label contains 81 information components, covering the CSP (e.g. physical location, legal jurisdiction), the cloud service itself (e.g. data location, security, backup, certification), and a historical service-level summary (e.g. uptime data, support response times). The label both provides data on the service and access to data. As such, it is in itself a form of cloud transparency mechanism (and has been extended to include the CSA CTP in to it [58]) and incorporates other trust mechanisms including third party assurances (certification) and SLA-verification (through the historical service-level summary).

This study explores the efficacy of the aforementioned CTL developed by [18] in building trust. The label aims to provide consumers with sufficient information about the service and service provider to allow them to make knowledge based trust decisions. In this paper, we explore the impact of the label on the trust related perceptions of consumers. We propose that the label will influence

consumers' initial perceptions of the cloud service and CSP and that this influence will be different depending on the information contained within the label.

Specifically, we hypothesise:

H1a The CTL will impact consumer perceptions of the trustworthiness (reliability, functionality and helpfulness) of a cloud service such that exposure to a label with positive information will increase trustworthiness perceptions and exposure to a label with negative information will decrease trustworthiness perceptions.
H1b The CTL will impact consumer trust in the cloud service such that exposure to a label with positive information will increase trust and exposure to a label with negative information will decrease trust.
H2a. The CTL will impact consumer perceptions of the trustworthiness (ability, benevolence and integrity) of a CSP such that exposure to a label with positive information will increase trustworthiness perceptions and exposure to a label with negative information will decrease trustworthiness perceptions.
H2b. The CTL will impact consumer trust in the CSP such that exposure to a label with positive information will increase trust and exposure to a label with negative information will decrease trust.

Methodology

Study design

To investigate the impact of the CTL on consumers' trust perceptions, we used an experimental design with a two label conditions – one positive and one negative. Participants were randomly assigned to one of the two conditions and completed the survey-based experiment online and in their own time. Participants were first presented with a description of a fictional cloud computing company called Cloud Solutions and their product, a cloud-based CRM system.[1] Participants were then asked to complete an online survey indicating their initial perceptions of the product and the provider. Following this initial survey, participants were presented with the CTL. Participants assigned to the positive condition were presented with a label which displayed positive information about the product including data security, data location and customer service quality level. These information points represent some of the factors impacting trust in the cloud context as highlighted by [74]. Participants in the negative condition were presented with a label which reported negative information about the same categories. As such, the independent variable in our study was the information contained in the label which we manipulated to be positive in one condition and negative in the other. The dependent variables in our study are perceptions of the product and provider which will be discussed in detail below.

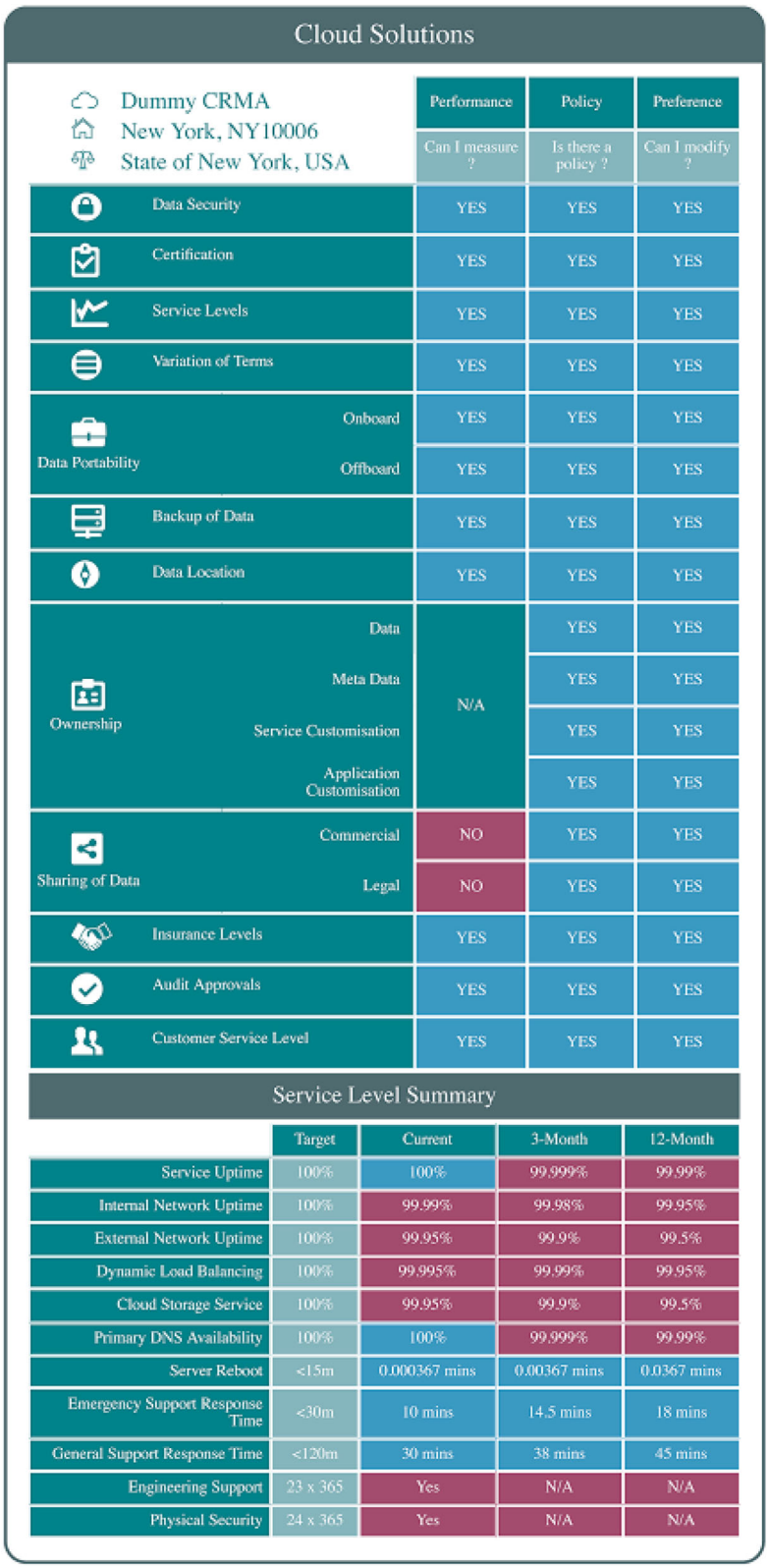
The experiment was designed to include both positive and negative conditions for two reasons. First, the inclusion of a negative condition allows us to investigate if any observed changes in trust are due to a learning effect based on repeated exposure to the trust measures or a response to the information contained within the label. Second, guidance for the design of experiments involving human subjects suggests that experimental variation should be maximised and that the difference between conditions for a given variable should be as large as possible while reflecting levels possible in the real world [75]. While CSPs may be unlikely to display a negative label, institutional authorities are likely to be more objective. Care was taken in the design of the labels to ensure that both positive and negative values were rooted in real-world levels. The positive and negative labels included in the experiment can be seen in Figs. 1 and 2. Immediately following their consideration of the additional information contained within the label interface, participants were asked to complete a second online survey to assess any change in their perceptions of the product and provider.

Cloud trust label content

As displayed in Figs. 1 and 2, the CTL specifies a range of important metrics identified as important in communicating trustworthiness to consumers of cloud services [18]. The CLT label is divided into three key parts: (i) details of the CSP including name, address and jurisdiction, (ii) the main section, and (iii) the service level summary. The main section of the CTL is divided into three further categories organising information according to whether it relates to the ability to measure a metric (Performance), the CSP's policy regarding a metric (Policy), and the extent to which the consumer can specify preferences for how a metric is dealt with (Preference). In each case, the value specified is designed to provide pop up links that give further details and or clarification. In this main section of the label information is provided on issues related to service execution and operational performance, data management, and contract conditions. The final section of the label provides a service level summary that includes further, more fine-grained details regarding the service level composite metric provided in the main section.

Participants

A population of marketing and IT professionals in Ireland and the UK were recruited for participation in the study using a purposive sampling strategy. Given the cloud service selected for use in the experiment this population was deemed suitable as these professionals are likely to be involved in the decision-making process for purchasing a CRM system. Potential participants were screened according to whether they were responsible for making the decision to purchase cloud-based software



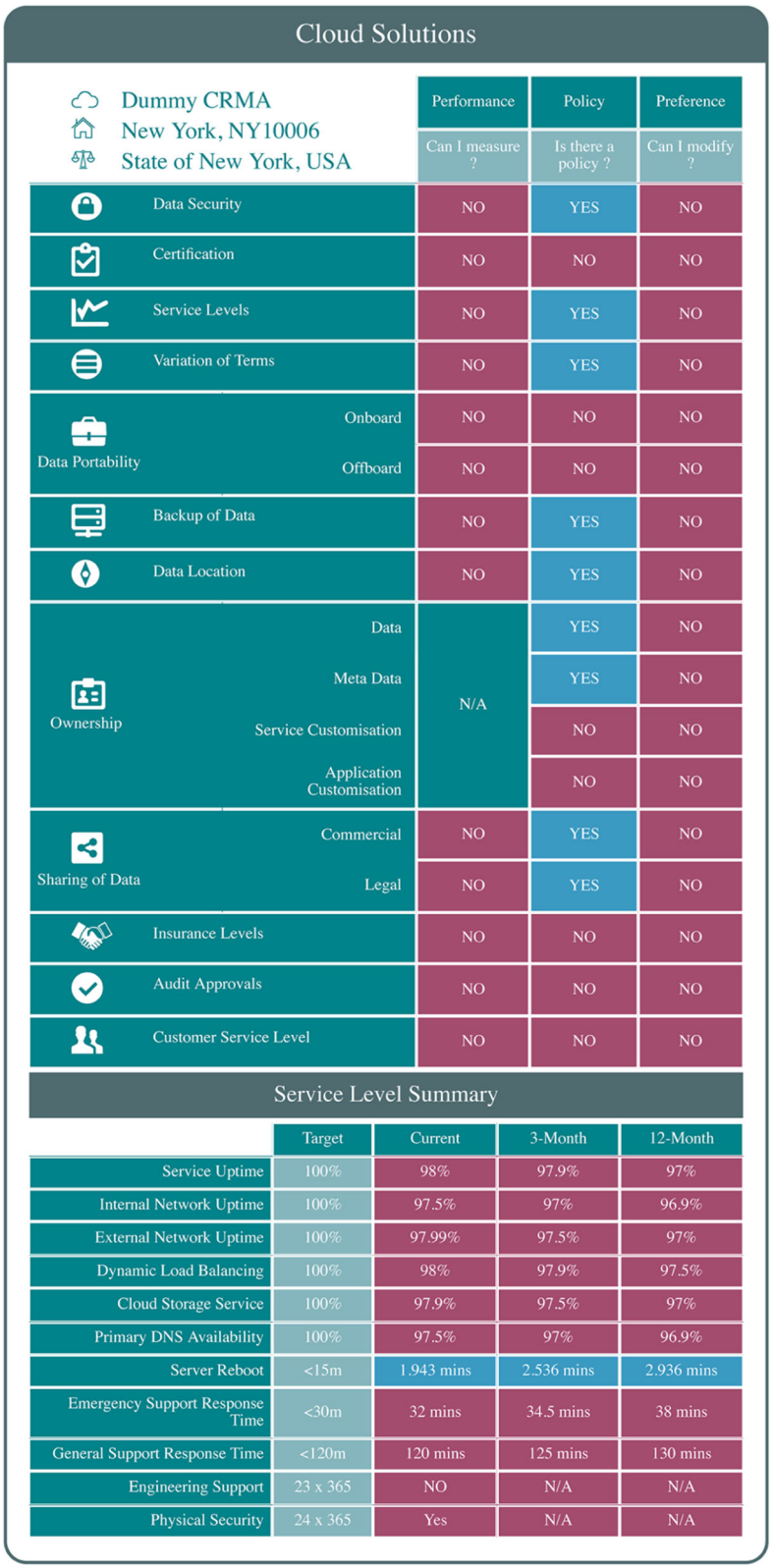
Cloud Solutions

Dummy CRMA New York, NY10006 State of New York, USA		Performance Can I measure ?	Policy Is there a policy ?	Preference Can I modify ?
Data Security		YES	YES	YES
Certification		YES	YES	YES
Service Levels		YES	YES	YES
Variation of Terms		YES	YES	YES
Data Portability	Onboard	YES	YES	YES
	Offboard	YES	YES	YES
Backup of Data		YES	YES	YES
Data Location		YES	YES	YES
Ownership	Data	N/A	YES	YES
	Meta Data		YES	YES
	Service Customisation		YES	YES
	Application Customisation		YES	YES
Sharing of Data	Commercial	NO	YES	YES
	Legal	NO	YES	YES
Insurance Levels		YES	YES	YES
Audit Approvals		YES	YES	YES
Customer Service Level		YES	YES	YES

Service Level Summary

	Target	Current	3-Month	12-Month
Service Uptime	100%	100%	99.999%	99.99%
Internal Network Uptime	100%	99.99%	99.98%	99.95%
External Network Uptime	100%	99.95%	99.9%	99.5%
Dynamic Load Balancing	100%	99.995%	99.99%	99.95%
Cloud Storage Service	100%	99.95%	99.9%	99.5%
Primary DNS Availability	100%	100%	99.999%	99.99%
Server Reboot	<15m	0.000367 mins	0.00367 mins	0.0367 mins
Emergency Support Response Time	<30m	10 mins	14.5 mins	18 mins
General Support Response Time	<120m	30 mins	38 mins	45 mins
Engineering Support	23 x 365	Yes	N/A	N/A
Physical Security	24 x 365	Yes	N/A	N/A

Fig. 1 Exemplar Positive CTL. An exemplar positive CTL was developed to explore the influence of positive information regarding the CSP on individuals' trust perceptions



Cloud Solutions

Dummy CRMA New York, NY10006 State of New York, USA		Performance Can I measure ?	Policy Is there a policy ?	Preference Can I modify ?
Data Security		NO	YES	NO
Certification		NO	NO	NO
Service Levels		NO	YES	NO
Variation of Terms		NO	YES	NO
Data Portability	Onboard	NO	NO	NO
	Offboard	NO	NO	NO
Backup of Data		NO	YES	NO
Data Location		NO	YES	NO
Ownership	Data	N/A	YES	NO
	Meta Data		YES	NO
	Service Customisation		NO	NO
	Application Customisation		NO	NO
Sharing of Data	Commercial	NO	YES	NO
	Legal	NO	YES	NO
Insurance Levels		NO	NO	NO
Audit Approvals		NO	NO	NO
Customer Service Level		NO	NO	NO

Service Level Summary

	Target	Current	3-Month	12-Month
Service Uptime	100%	98%	97.9%	97%
Internal Network Uptime	100%	97.5%	97%	96.9%
External Network Uptime	100%	97.99%	97.5%	97%
Dynamic Load Balancing	100%	98%	97.9%	97.5%
Cloud Storage Service	100%	97.9%	97.5%	97%
Primary DNS Availability	100%	97.5%	97%	96.9%
Server Reboot	<15m	1.943 mins	2.536 mins	2.936 mins
Emergency Support Response Time	<30m	32 mins	34.5 mins	38 mins
General Support Response Time	<120m	120 mins	125 mins	130 mins
Engineering Support	23 x 365	NO	N/A	N/A
Physical Security	24 x 365	Yes	N/A	N/A

Fig. 2 Exemplar Negative CTL. An exemplar negative CTL was developed to explore the influence of negative information regarding the CSP on individuals' trust perceptions

such as CRM systems. Participants who indicated that they do not hold responsibility for such decisions were excluded from the study. It should be noted that this population of decision makers hold business expertise and responsibility but are unlikely to hold significant technical expertise with regards to the functioning of cloud services and technology. On this basis, 227 respondents were then selected for participation out of a total number of 367 participants contacted, representing a response rate of 62%. The recruitment and screening process was identical for both conditions.

The final sample was 70.94% male and 57% of participants reported being between the ages of 30 and 49. The majority of participants (73.1%) had attended third level education and attained a bachelor (33.9%) or masters (39.2%) degree. The sample was drawn from a range of organisational sizes with 16.7% working in micro sized organisations (1–9 employees), 15.9% working in small organisations (10–49 employees), 27.8% working in medium sized organisations (50–249 employees) and 33% working in large organisations (more than 250 employees). Almost two thirds (62.6%) of the population reported that their organisation already had a CRM system.

Measures

All measures employed in the survey were based on validated scales from prior research. All items were measured on a 5-point Likert scale and anchors were varied across variables in line with the original scales and to help prevent common method bias [75].

Cloud service variables

To measure perceptions of cloud service trustworthiness we adapted an 11-item measure developed by [76] to assess the reliability (4 items), functionality (3 items) and helpfulness (4 items) of an IT artefact. Samples items for the sub dimensions are "This service is a very reliable piece of technology", "This service has the functionality I need", and "This service provides whatever help I need" respectively. The scale demonstrated acceptable internal consistency with Cronbach's alpha values ranging from .91–.93 across pre and post label measurement points. Trust in the cloud service was measured using a 4-item scale adapted from Mayer and Gavin's [77] scale. A sample item is "I would be comfortable relying on this cloud service for something that was critical to me, even if I couldn't monitor its actions". The scale demonstrated acceptable internal consistency at pre and post label measurement points (pre, α = .92; post, α = .91).

CSP variables

CSP trustworthiness was operationalised using 17 items adapted from a scale developed by [78]. The scale contains three sub dimensions: ability (6 items), benevolence (5 items) and integrity (6 items). Samples items for each of the subscales are as follows "Cloud Solutions is very capable of providing an excellent service", "My needs and desires are very important to Cloud Solutions", and "Cloud Solutions tries hard to be fair in dealing with customers". The internal consistency for each of the subscales was acceptable with Cronbach's alpha values ranging from .89 to .94 across both time points. We assessed trust in the CSP 4 items adapted from [77]. A sample items is "If someone questioned Cloud Solutions' motives, I would give them the benefit of the doubt". This scale demonstrated acceptable consistency with a Cronbach's alpha of .87 at the pre-label measurement point and .89 at the post-label measurement point.

Other variables

We collected data on a number of additional demographic and dispositional variables which may impact participant ratings of trust perceptions. In addition to demographic data regarding gender and age, we also collected data on whether respondents currently have a CRM system and whether they believe the cloud is a suitable platform for a CRM system. We collected data on participants' propensity to trust (PTT) others using MacDonald and colleague's [79] 10-item measure. A sample item is "I am more trusting than a lot of people". Finally, we used the 7-item scale developed by Mc Knight et al. [76] to measure propensity to trust technology (PTTT). A sample item is "I usually trust a technology until it gives me a reason not to trust it". Both propensity scales demonstrated acceptable internal consistency (α = .70 and α = .90 respectively).

Results

Statistical analyses were conducted using SPSS version 21. To compare participants across conditions and confirm random assignment, a series of independent sample t-tests and chi square tests were conducted on demographic and dispositional variables. The results indicated that participants in the positive and negative label conditions did not differ across gender, current ownership of a CRM system, belief that the cloud is an appropriate platform for CRM systems, propensity to trust or propensity to trust technology. The Harman single factor test indicated that a single method factor cannot explain the majority of the variance in our variables (38%) and that common method bias is not a major concern in this instance. Hypotheses were tested using a series of repeated measures ANOVAs (RMANOVA). This method is suitable for detecting within-subject change in dependent variables. In this instance we are interested to investigate within-subject change in perceptions of trustworthiness and trust between the pre-label and post-label conditions. The Type 1 error rate was set at .05 and missing data was dealt with using a listwise deletion approach.

Table 2 Correlations and Descriptive Statistics for Key Study Variables

	M	SD	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
T1 Ability	3.55	0.81	(.93)																	
T1 Benevolence	3.33	0.85	.78*	(.92)																
T1 Integrity	3.30	0.62	.83*	.81*	(.89)															
T1 ProviderTrust	3.26	0.91	.72*	.67*	.72*	(.88)														
T1 Reliability	3.34	0.87	.80*	.70*	.72*	.73*	(.92)													
T1 Functionality	3.54	0.88	.79*	.63*	.71*	.62*	.82*	(.92)												
T1 Helpfulness	3.43	0.83	.80*	.70*	.76*	.72*	.87*	.82*	(.92)											
T1 CloudServiceTrust	3.28	0.93	.77*	.68*	.73*	.84*	.85*	.76*	.83*	(.91)										
T2 Ability	3.45	0.85	.70*	.59*	.65*	.60*	.75*	.70*	.74*	.73*	(.94)									
T2 Benevolence	3.32	0.86	.63*	.70*	.67*	.61*	.67*	.60*	.70*	.70*	.81*	(.92)								
T2 Integrity	3.29	0.61	.63*	.61*	.67*	.64*	.70*	.65*	.74*	.71*	.83*	.84*	(.90)							
T2 ProviderTrust	3.29	0.85	.62*	.58*	.63*	.70*	.75*	.63*	.70*	.78*	.87*	.82*	.85*	(.89)						
T2 Reliability	3.35	0.91	.62*	.58*	.57*	.63*	.72*	.64*	.70*	.72*	.86*	.78*	.81*	.85*	(.91)					
T2 Functionality	3.41	0.89	.63*	.55*	.63*	.58*	.65*	.64*	.66*	.68*	.80*	.73*	.77*	.76*	.74*	(.93)				
T2 Helpfulness	3.37	0.86	.61*	.55*	.64*	.62*	.66*	.62*	.70*	.70*	.81*	.76*	.81*	.81*	.78*	.77*	(.93)			
T2 CloudServiceTrust	3.25	0.92	.68*	.62*	.65*	.75*	.72*	.60*	.71*	.80*	.83*	.79*	.80*	.91*	.86*	.78*	.83*	(.91)		
PTT	3.19	0.52	.18*	.07	.16*	.14*	.19*	.17*	.08	.12	.06	.02	.08	.12	.03	.07	.06	.12	(.81)	
PTTTechnology	3.55	0.74	.66*	.58*	.61*	.53*	.63*	.63*	.64*	.62*	.70*	.65*	.62*	.63*	.62*	.64*	.64*	.67*	.25*	(.90)

aCoefficient alpha reliability estimates are in parentheses.
*$p < .05$

Descriptive statistics and correlational analysis was carried out on the key variables of interest at both measurement points. The means (M), standard deviations (SD) and correlations are displayed in Table 2 above to provide details of the patterns of responses to and relationships between our variables of interest.

Cloud service perceptions

The results of RMANOVAs for the impact of the label of reliability, functionality and helpfulness perceptions of the cloud service indicated partial support for Hypothesis 1a. A significant interaction effect between time and label condition was found for helpfulness perceptions (Wilks' Lambda = .97, F = 5.32, $p < .05$). In addition, significant between person effects were found for perceptions of helpfulness ($F = 4.88$, $p < .05$) and reliability ($F = 4.36$, $p < .05$). No significant differences were seen for functionality. Changes across conditions and over time can be seen in Figs. 3, 4 and 5 which indicate that perceptions of functionality decrease over time for both conditions while perceptions of helpfulness and reliability increase for the positive label condition and decrease for the negative label condition. Post hoc t-tests revealed that while there were no differences between group means of reliability (t (211) = 1.42, $p > .05$), functionality (t (210) = .47, $p > .05$) and helpfulness (t (211) = 1.01, $p > .05$) at pre-label data collection, the means of the groups were significantly different on all three variables (reliability t (207) = 2.51, $p < .05$; functionality t (205) = 2.17, $p < .05$; helpfulness t (206) = 2.94, $p < .05$) at the post-label time point.

To test Hypothesis 1b regarding the impact of the label on trust in the cloud service another RMANOVA was conducted. Results demonstrate a significant interaction effect between time and label condition for within person trust in the product (Wilks' Lambda = .98, $F = 5.05$, $p < .05$) as well as significant between person effects ($F = 6.78$, $p < .05$). Figure 6 illustrates the increase over time for participants exposed to the positive label and a decrease over time for participants exposed to the negative label. Again, post hoc t-tests indicate that there were no significant differences between the positive and negative conditions at time 1 (t (210) = 1.79, $p > .05$) but the differences between groups at time 2 were significant (t (206) = 2.88, $p < .05$).

CSP perceptions

Analysis indicated partial support for Hypothesis 2a which stated that the label would have an impact on consumer perceptions of CSP trustworthiness. Wilks' Lambda estimates showed a significant interaction between label condition and time for within person perceptions of CSP ability (Wilks' Lambda = .98, $F = 4.09$, $p < .05$) but not for benevolence or integrity. All three trustworthiness perceptions showed significant between person effects (ability, $F = 7.72$, $p < .05$; benevolence, $F = 3.91$, $p < .05$; integrity, $F = 5.26$, $p < .05$). As can be seen in Fig. 7, participants in the

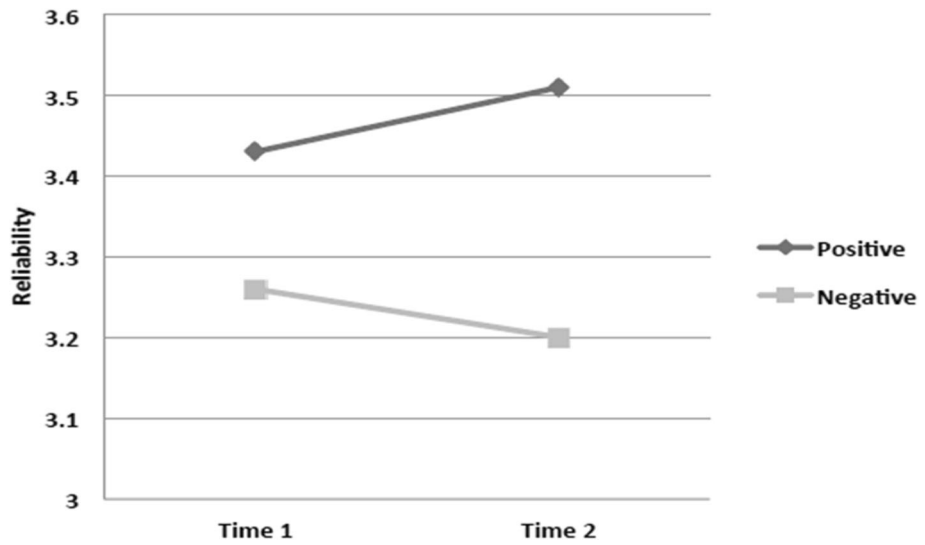


Fig. 3 Reliability means by condition at Time 1 and Time 2. The figure shows the difference in the mean perception of reliability between time 1 prior to exposure to the label and time 2 after exposure to the label. As shown, the positive label increased perceptions of reliability, whereas exposure to the negative label reduced perceptions of reliability

positive condition showed relatively stable perceptions of ability over time while those in the negative condition decreased. Post hoc analysis confirms that this change was significant for the negative label group (t (101) = 3.21, $p < .05$) but non-significant for the positive label group (t (99) = .46, $p > .05$). In contrast, benevolence and integrity perceptions show increases after label presentation for the positive label condition and decreases after label presentation for the negative label condition (Figs. 8 and 9). Post hoc comparisons reveal that differences between respondents in the positive condition and those in the negative condition are non-significant at time 1 (ability t (220) = 1.34, $p > .05$; benevolence t (215) = .94, $p > .05$; integrity t (218) = 1.27, $p > .05$). After respondents had been exposed to the label differences between the groups was significant for ability (t (205) = 3.24, $p < .05$), benevolence (t (207) = 2.67, $p < .05$) and integrity (t (204) = 2.61, $p < .05$).

Hypothesis 2b stated that presentation of the label should impact consumer trust in the CSP. RMANOVA

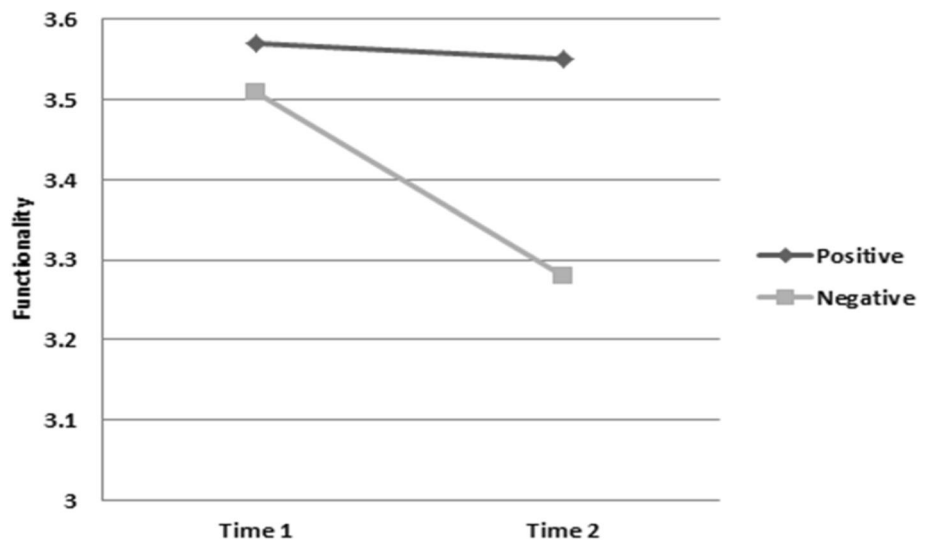


Fig. 4 Functionality means by condition at Time 1 and Time. The figure shows the difference in the mean perception of functionality between time 1 prior to exposure to the label and time 2 after exposure to the label. As shown, exposure to both label conditions reduced perceptions of functionality. However, this effect was far more drastic for the negative label condition, with perceived functionality reducing dramatically

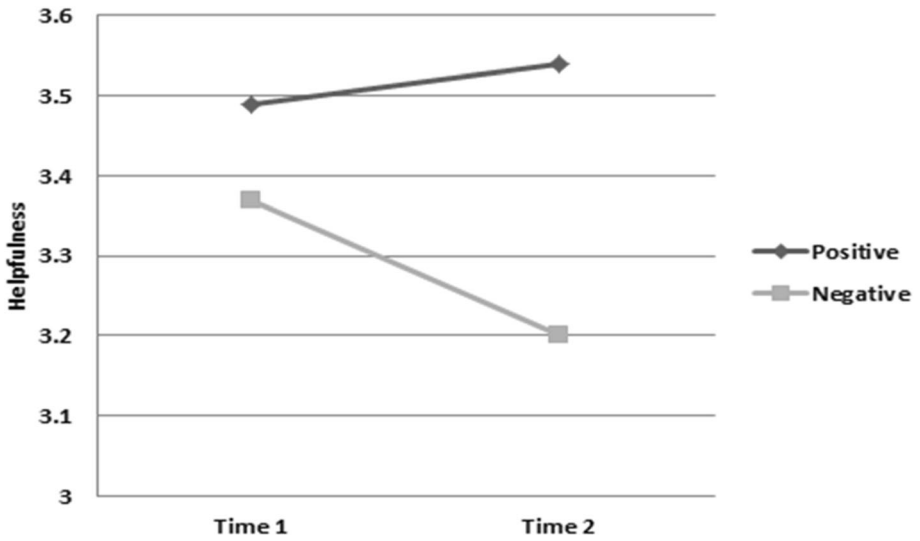


Fig. 5 Helpfulness means by condition at Time 1 and Time 2. The figure shows the difference in the mean perception of helpfulness between time 1 prior to exposure to the label and time 2 after exposure to the label. As shown, the positive label increased perceptions of helpfulness, whereas exposure to the negative label reduced perceptions of helpfulness

demonstrated a significant between subject effect for experimental condition ($F = 5.01$, $p < .05$). As seen in Fig. 10, participants in the positive condition showed increases in trust in the CSP over time while those in the negative condition showed decreases in trust. Independent samples t-tests indicate that differences between groups were non-significant at pre-label measurement (t (224) = 1.01, $p > .05$) and significant at post-label measurement (t (203) = 2.58, $p < .05$).

Discussion

The aim of this paper was to investigate the impact of a CTL on consumer perceptions of a common business-to-business cloud-based SaaS offering, in this case a CRM system. The results of this experimental study suggest that a cloud computing trust label can provide an effective means of communicating trustworthiness to business consumers and assisting consumers in differentiating meaningfully between SaaS cloud computing services. As

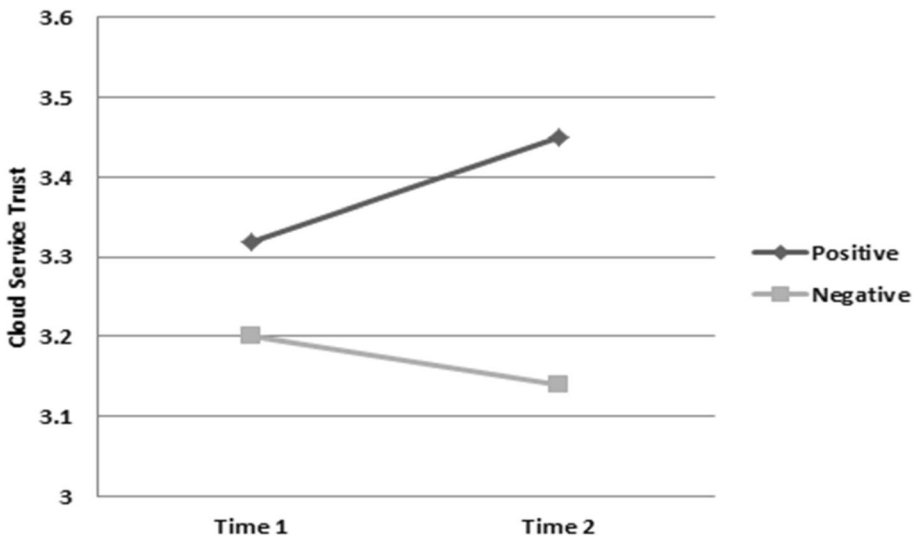


Fig. 6 Cloud Service Trust means by condition at Time 1 and Time 2. The figure shows the difference in overall trust in the cloud service between time 1 prior to exposure to the label and time 2 after exposure to the label. As shown, the positive label increased trust in the cloud service, whereas exposure to the negative label reduced trust

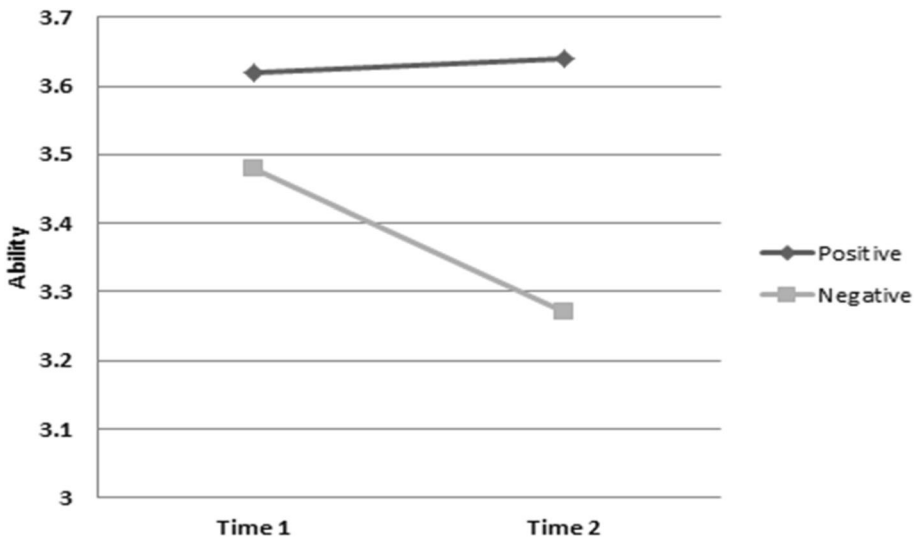


Fig. 7 Ability means by condition at Time 1 and Time 2. The figure shows the difference in perceptions of ability between time 1 prior to exposure to the label and time 2 after exposure to the label. As shown, exposure to the positive label led to a slight increase in perceived ability, whereas exposure to the negative label led to a big decrease in perceived ability

hypothesised, the results suggest that trust labels which contain positive information can have a positive impact on trust while trust labels containing negative information can have a negative impact on trust. As such, the study makes a significant contribution to the literature in extending the findings in relation to trustmarks in the e-commerce context to cloud computing and validating the impact for the trust label design [18]. The validation of the CTL also represents a significant contribution to practice and a method for CSPs or institutional authorities in the Cloud industry to communicate trust to consumers.

The findings suggest that the label impacts consumer perception of both the SaaS cloud service and the CSP. Our findings also indicate that the impact on consumer perceptions of trust and trustworthiness differs depending on whether the focus of trust is the cloud service itself or the provider. This is an important distinction as the majority of empirical work in the area has failed to account for

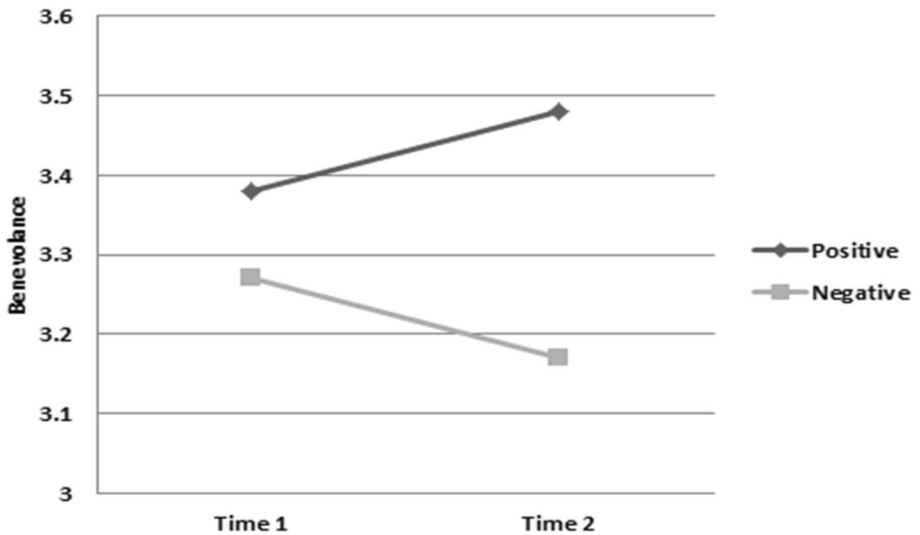


Fig. 8 Benevolence means by condition at Time 1 and Time 2. The figure shows the difference in perceptions of benevolence between time 1 prior to exposure to the label and time 2 after exposure to the label. As shown, exposure to the positive label led to an increase in perceptions of benevolence, whereas exposure to the negative label decreased perceived benevolence

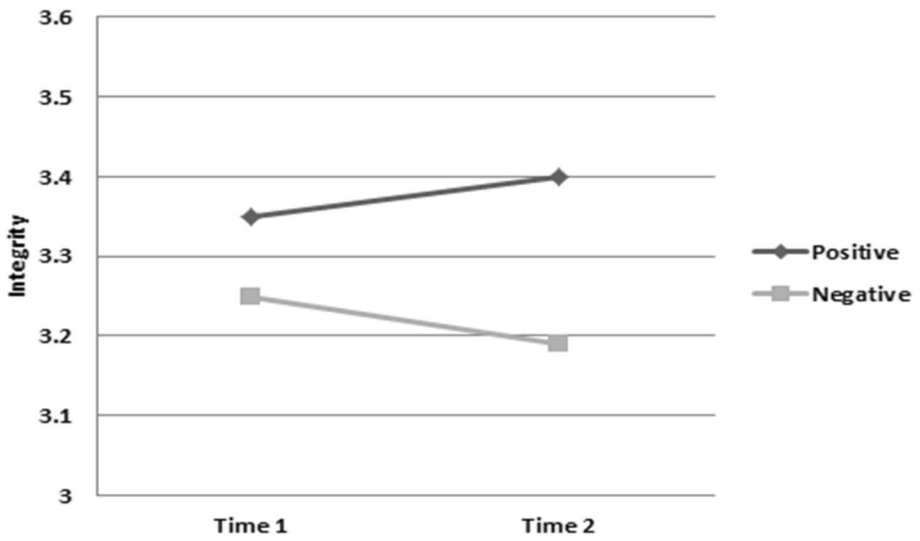


Fig. 9 Integrity means by condition at Time 1 and Time 2. The figure shows the difference in perceptions of integrity between time 1 prior to exposure to the label and time 2 after exposure to the label. As shown, exposure to the positive label led to an increase in perceived integrity, whereas exposure to the negative label led to a decrease in perceived integrity

the existence of multiple referents in the cloud computing context given the chain of service provision [32]. These results provide support for the theoretical work of [40, 80] who argue that researchers in the field of information management need to differentiate between trust in IT artefacts and trust in organisations or individuals providing an IT service. Our research suggests that, for SaaS cloud computing, trust involves dimensions of both human and objectified trust and as such consumers' perceptions of service provider benevolence, integrity, and ability [41] and cloud service reliability, functionality and helpfulness [76]. In doing so, our research answers recent calls for more contextualised research in the area of trust in cloud computing and provides support for theory which proposes multiple referents play a role in this environment [32].

More broadly, our research informs trust theory [41, 47] by demonstrating a method for building knowledge-based trust without a history of interactions between parties in a business relationship. Within the field of information systems, attempts to build trust without a history of

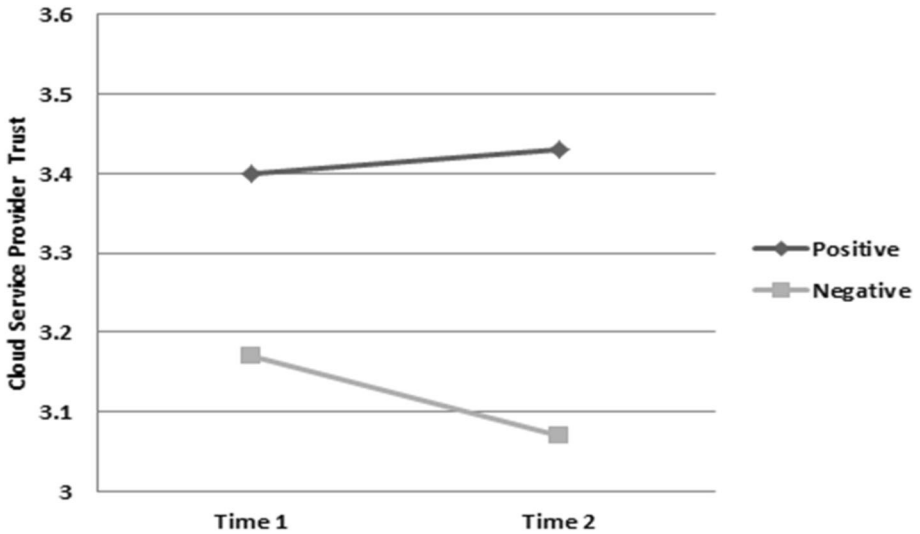


Fig. 10 CSP Trust means by condition at Time 1 and Time 2. The figure shows the difference in trust in the CSP between time 1 prior to exposure to the label and time 2 after exposure to the label. As shown, exposure to the positive label led to a slight increase in CSP Trust, whereas exposure to the negative label led to a decrease in CSP Trust

interactions have tended to focus on third party information (e.g. recommendation systems) or heuristic cues (e.g. website design). We argue that by providing objective information about the service itself, the CTL offers an opportunity to bypass suspicious, fragile forms of calculative trust and build more robust, knowledge-based trust with consumers from the very beginning of a relationship. As such the research makes empirical and theoretical contributions to literature on trust in the cloud by moving beyond studies which highlight the importance of trust to building a means for fostering trust in this complex environment. The study's findings are also of critical importance to practice not only echoing the assertions of prior researchers [31] for organisations to develop approaches for increasing perceptions of trust, but also presenting the CTL as a means of doing so.

Limitations and future research

This research was conducted using an experimental design, this methodological choice was appropriate for a validation study as it offers the advantage of isolating the manipulation of label information from a host of other potentially influencing variables. However, experimental designs lack the naturalistic features of a field study and this research represents a validation of the label in a relatively artificial environment. This limitation was offset to some extent by careful screening of participants and the use of business decision makers as our sample. Future research is necessary to determine how cloud trust decisions might be influenced by more dynamic label information presented over a longer time frame including opportunities for time series analysis. Further work might also explore how this information interacts with other perceptions of the service or service provider such as brand, reputation and third-party knowledge.

The focus of this study was on validating the impact of the CTL on consumer trust. The design of this label was based on the assumption that providing consumers with additional, relevant information is likely to provide a more meaningful means of communicating trustworthiness than existing approaches. Further research is necessary to demonstrate the impact of the label in comparison to alternative more implicit measures such as assurance seals or website design features within the cloud environment. Furthermore, the relative influence of trust in each referent in terms of impact on subsequent behaviour is a potentially fruitful area for further research. Trust theory would suggest that trust follows a universal three stage process [46, 81] whereby trustworthiness perceptions influence trust and subsequently trust behaviour. It is less clear how the existence of multiple referents in the cloud environment would interact to influence consumer risk taking behaviours such as purchasing decisions, but this certainly represents an interesting avenue for future research.

Our experiment focused on only one type of SaaS offering, a CRM system, and largely business decision-makers. CRM systems have consistently been in the most commonly adopted SaaS services by businesses of all sizes worldwide, primarily due to the seminal impact of Salesforce.com in the cloud computing industry. Furthermore, CRM users and decision makers are typically non-technical, typically sales and marketing executives. As such, our sampling strategy is consistent with other studies on CRM systems [82, 83]. Notwithstanding this, CRM systems are not representative of all SaaS-based systems, and CRM and SaaS decision-makers are not necessarily representative of PaaS, IaaS and other cloud offerings where adoption and usage is determined largely by technical end users and decision makers. As such, further research is warranted on the trust label data requirements for other cloud offerings and their associated audiences.

Finally, our experiment focuses on the overall impact of the label on trust related consumer perceptions. In a real-world setting, CTLs are likely to be populated with a range of positive and negative information rather than the simpler positive and negative conditions presented in this validation. The extent to which the manipulation of certain aspects of the label impacts consumer perceptions is a useful avenue for future work. We expect this will be a highly contextualised issue whereby particular aspects of the label will be more or less important for different products or indeed consumer markets. In addition, it may be that certain parts of the label are related to specific aspects of trustworthiness. For instance, service uptime may act as a signal of functionality of the service while data location provides a signal of benevolence of the service provider. Examining the intricacies of these relationships requires further study.

Conclusion

Cloud computing is forcing us to rethink our conceptualisation of data and technology ownership, usage and rights. It is also changing our relationship with the technology and technology provider and how we operationalise and communicate trust. The widespread adoption and dependency by both businesses and public-sector organisations on cloud computing, and so-called utility-computing, may have a knock-in effect on consumer expectations for continuity and service levels. In much the same way, we trust electricity, water and telecommunications suppliers and ascribe a higher level of duty of care to them and by association, trust, we may also treat CSPs in the future. If trustworthiness in online environments is a signalling-based phenomenon driven by information transparency then the proposed cloud label, particularly if real-time and dynamic, would represent a significant step in the evolution of cloud computing in the same way the nutritional label has done so in the modern food industry.

Endnotes

[1]Both labels were developed using best practice in label design as discussed further in [18]).

Abbreviations

CRM: Customer Relationship Management System; CSP: Cloud Service Provider; CTL: Cloud Trust Label; IaaS: Infrastructure as a Service; IT: Information Technology; NIST: National Institute of Standards and Technology; PaaS: Platform as a Service; PTT: Propensity to Trust; PTTT: Propensity to Trust Technology; SaaS: Software as a Service

Acknowledgements

The research work described in this paper was supported by the Irish Centre for Cloud Computing and Commerce, an Irish National Technology Centre funded by Enterprise Ireland and the Irish Industrial Development Authority.

Funding

This research was supported by the Irish Centre for Cloud Computing and Commerce, an Irish National Technology Centre funded by Enterprise Ireland and the Irish Industrial Development Authority.

Availability of data and materials

Data will not be shared as the authors do not have permission to share data from the study.

Authors' contributions

LvdW designed the survey, performed the statistical analyses and led the write up of the manuscript. GF contributed to the writing of the manuscript. IM contributed to the statistical analyses. TL conceived the study and helped coordinate the data collection efforts. VE and JM led the development of the trust labels. All authors read and approved the manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

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

Author details

[1]Irish Institute of Digital Business, Dublin City University Business School, Dublin, Ireland. [2]Irish Centre for Cloud Computing and Commerce, Dublin City University, Dublin, Ireland. [3]Department of Computer Science, Cork Institute of Technology, Cork, Ireland. [4]Irish Centre for Cloud Computing and Commerce, University College Cork, Cork, Ireland.

Received: 25 September 2018 Accepted: 8 April 2019
Published online: 24 April 2019

References

1. National Institute of Standards and Technology (2009). The NIST definition of cloud computing. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf. Accessed 14 June 2018
2. Lynn T, Liang X, Gourinovitch A, Morrison JP, Fox G, Rosati P (2018) understanding the determinants of cloud computing adoption for high performance computing. In: Proceedings of the 51st Hawaii international conference on system sciences (HICSS-51). University of Hawai'i at Manoa, Hawaii, pp 3–6
3. Arpaci I (2016) Understanding and predicting students' intention to use mobile cloud storage services. Comput Hum Behav 58:150–157
4. Yu Y, Li M, Hao J, Li X, Zhao LJ (2017) Mediating role of trust brief in SMEs' strategic choice of cloud service. In: Proceedings of the twenty-third Americas conference on information systems, Boston, pp 10–12
5. Rosati P, Fox G, Kenny D, Lynn T (2017) Quantifying the financial value of cloud investments: a systematic literature review. In Proceedings of the 2017 IEEE international conference on cloud computing technology and science (CloudCom), Hong Kong
6. Gartner (2017) Forecast: public cloud services, worldwide, 2014–2020, 4Q16 Update. https://www.gartner.com/doc/3562817/forecast-public-cloud-services-worldwide. Accessed 12 June 2018
7. Stankov I, Datsenka R, Kurbel K (2012) Service level agreement as an instrument to enhance trust in cloud computing–an analysis of infrastructure-as-a-service providers. In: Proceedings of the eighteenth Americas conference on information systems, Seattle, pp 9–12
8. Hwang K, Li D (2010) Trusted cloud computing with secure resources and data coloring. Internet Computing, IEEE 14(5):14–22
9. Rousseau DM, Sitkin SB, Burt RS, Camerer C (1998) Not so different after all: a cross-discipline view of trust. Acad Manag Rev 23(3):393–404
10. Grabner-Kräuter S, Kaluscha EA (2003) Empirical research in on-line trust: a review and critical assessment. Int J Hum Comput Stud 58(6):783–812
11. Corritore CL, Kracher B, Wiedenbeck S (2003) On-line trust: concepts, evolving themes, a model. Int J Hum Comput Stud 58(6):737–758
12. Wang W, Benbasat I (2008) Attributions of trust in decision support technologies: a study of recommendation agents for e-commerce. J Manag Inf Syst 24(4):249–273
13. Silic M, Barlow J, Back A (2018) Evaluating the role of Trust in Adoption: a conceptual replication in the context of open source systems. AIS Transactions on Replication Research 4:1):1–1)17
14. Roghanizad MM, Neufeld DJ (2015) Intuition, risk, and the formation of online trust. Comput Hum Behav 50:489–498
15. Inbar Y, Cone J, Gilovich T (2010) People's intuitions about intuitive insight and intuitive choice. J Pers Soc Psychol 99(2):232
16. Lankton NK, McKnight DH, Tripp J (2015) Technology, humanness, and trust: rethinking trust in technology. J Assoc Inf Syst 16(10):880
17. Cusack B, Ghazizadeh E (2016) Formulating methodology to build a trust framework for cloud identity management. In: Proceedings of the twenty-second Americas conference on information systems, San Diego, pp 11–14
18. Lynn T, van der Werff L, Hunt G, Healy P (2016) Building user trust in the cloud: a nutritional label for signalling trustworthiness. J Comput Inf Syst 56(3):185–193
19. Huang J, Nicol DM (2013) Trust mechanisms for cloud computing. J Cloud Comput 2(9):9
20. Jie Z, Zhang JA, Wen J (2010) trust evaluation model based on cloud model for C2C electronic commerce. In Computer application and system modelling (ICCASM), Taiyuan
21. Yang Y, Chen J (2009) a dynamic trust evaluation model on C2C marketplaces. In Computational science and engineering, Miami
22. Habib SM, Hauke S, Ries S, Muhlhauser M (2012) Trust as a facilitator in cloud computing: a survey. Journal of Cloud Computing 1(1):19
23. Paward P, Rajarajan M, Nair S, Zisman A (2012) Trust model for optimized cloud services. In: IFIP international conference on trust management 2012. Springer, Berlin, Heidelberg, pp 97–112
24. Kelley GK, Bresee J, Cranor LF, Reeder RW (2009) a nutrition label for privacy. In Proceedings of the 5th symposium on usable privacy and security, mountain view
25. Kelley GK, Cesca L, Bresee J, Craner LF (2010) Standardizing privacy notices: an online study of the nutrition label approach. In: Proceedings of the SIGCHI conference on human factors in computing systems, Atlanta
26. Abawajy J (2011) Establishing trust in hybrid cloud computing environments. In: 2011 IEEE 10th international conference on trust, security and privacy in computing and communications. IEEE, pp 118–125
27. Weick KE (1995) Sensemaking in organizations, foundations for organizational science. Sage, Thousands Oaks
28. Lewis JD, Weigert A (1985) Trust as a social reality. Social Forces 63(4):967–985
29. McKnight DH, Choudhury V, Kacmar C (2002) Developing and validating trust measures for e-commerce: an integrative typology. Inf Syst Res 13(3):334–359
30. Jarvenpaa SL, Shaw TR, Staples DS (2004) Toward contextualized theories of trust: the role of trust in global virtual teams. Inf Syst Res 15(3):250–267
31. Moqbel MA, Bartelt VA (2015) Consumer acceptance of personal cloud: integrating trust and risk with the technology acceptance model. Transactions on Replication Research 1:1–11
32. Lansing J, Sunyaev A (2016) Trust in Cloud Computing: conceptual typology and trust-building antecedents. ACM SIGMIS Database 47(2):58–96
33. Luftman J, Zadeh HS, Derksen B, Santana M, Rigoni EH, Huang ZD (2013) Key information technology and management issues 2012–2013: an international study. J Inf Technol 28(4):354–366
34. Asatiani A (2015) Why Cloud? – A Review of Cloud Adoption Determinants in Organizations. In Proceedings of the 23rd European Conference on Information Systems, Muenster

35. Hew TS, Kadir SLSA (2016) Behavioural intention in cloud-based VLE: an extension to channel expansion theory. Comput Hum Behav 64:9–20
36. Gefen D, Karahanna E, Straub DW (2003) Trust and TAM in online shopping: an integrated model. MIS Q 27(1):51–90
37. Pavlou P, Gefen D (2004) Building effective online marketplaces with institution based trust. Inf Syst Res 15(1):37–59
38. Everard A, Galletta DF (2005) How presentation flaws affect perceived site quality, trust, and intention to purchase from an online store. J Manag Inf Syst 22(3):56–95
39. Bente G, Baptist O, Leuschner H (2012) To buy or not to buy: influence of seller photos and reputation on buyer trust and purchase behaviour. Int J Hum Comput Stud 70(1):1–13
40. McKnight DH (2005) Trust in information technology. The Blackwell Encyclopaedia of Management 7:329–331
41. Mayer RC, Davis JH, Schoorman FD (1995) An integrative model of organizational trust. Acad Manag Rev 20(3):709–734
42. Kim J, Moon JY (1998) Designing towards emotional usability in customer interfaces—trustworthiness of cyber-banking system interfaces. Interact Comput 10(1):1–29
43. Sillence E, Briggs P, Harris PR, Fishwick L (2007) How do patients evaluate and make use of online health information? Social Science Medicine 64(9):1853–1862
44. Cyr D, Head M, Larios H (2010) Colour appeal in website design within and across cultures: a multi-method evaluation. Int J Hum Comput Stud 68(1):1–21
45. Tuch AN, Bargas-Avila JA, Opwis K (2010) Symmetry and aesthetics in website design: It's a man's business. Comput Hum Behav 26(6):1831–1837
46. Dietz G (2011) Going back to the source: why do people trust each other? J Trust Res 1(2):215–222
47. Lewicki RJ, Bunker BB (1996) Developing and maintaining trust in work relationships. In: Kramer R, Tyler TR (eds) Trust in organizations: Frontiers of theory and research. Sage, Thousand Oaks, pp 114–139
48. Resnick P, Kuwabara K, Zeckhauser R, Friedman E (2000) Reputation systems. Commun ACM 43(12):45–48
49. Resnick P, Zeckhauser R (2002) Trust among strangers in internet transactions: empirical analysis of eBay's reputation system. The Economics of the Internet and E-commerce 11(2):23–25
50. Koster A, Schorlemmer M, Sabater-Mir J (2012) Opening the black box of trust: reasoning about trust models in a BDI agent. J Log Comput 23(1):25–58
51. Baldwin A, Pym D, Shiu S (2013) Enterprise information risk management: dealing with cloud computing. In: Pearson S, Yee G (eds) Privacy and security for cloud computing. Springer, London, pp 257–291
52. Hwang K, Kulkareni S, Hu Y (2009, December) Cloud security with virtualized defense and reputation-based trust mangement. In: Dependable, autonomic and secure computing, 2009. DASC'09. Eighth IEEE international conference on. IEEE, pp 717–722
53. Tan YH, Theon W (2001) Toward a generic model of trust for electronic commerce. Int J Electron Commer 5(2):61–74
54. Stewart KJ (2003) Trust transfer on the world wide web. Organ Sci 14(1):5–17
55. Kirlappos I, Sasse MA, Harvey N (2012) Why trust seals don't work: a study of user perceptions and behavior. In: Proceedings of the Iternational conference on trust and trustworthy computing, Vienna, pp 13–15
56. McKnight DH, Kacmar CH, Choudhury V (2004) Shifting factors and the ineffectiveness of third party assurance seals: a two-stage model of initial trust in a web business. Electron Mark 14(3):252–266
57. Haq IU, Alnemr R, Paschke A, Schikuta E, Boley H, Meinel C (2010) Distributed trust management for validating sla choreographies. In: Grids and service-oriented architectures for service level agreements. Springer, Boston, pp 45–55
58. Emeakaroha VC, O'Meara E, Lynn T, Lee B, Morrison J (2017) Establishing Trust in Cloud Services via Integration of Cloud Trust Protocol with a Trust Label System. In the Proceedings of CLOSER: The 7th International Conference on Cloud Computing and Services Science, Portugal
59. CSA (2011) Cloud Trust Protocol – Orientation and Status. https://cloudsecurityalliance.org/wp-uploads/2011/08/CloudTrust-Protocol.ppt. Accessed 25 Jan 2019
60. Dell EMC (2012) RSA and Zscaler Teaming Up to Deliver Trusted Access for Cloud Computing. https://www.emc.com/about/news/press/2012/20120228-02.htm. Accessed 25 Jan 2019
61. Xia Q, Sifah E, Smahi A, Amofa S, Zhang X (2017) BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information 8(2):44
62. Maitlis S, Christianson M (2014) Sensemaking in organizations: taking stock and moving forward. Acad Manag Ann 8(1):57–125
63. Garrison G, Kim S, Wakefield RL (2012) Success factors for deploying cloud computing. Commun ACM 55(9):62–68
64. Weick KE, Sutcliffe KM (2006) Mindfulness and the quality of organizational attention. Organ Sci 17(4):514–524
65. Lieberman MD (2007) Social cognitive neuroscience: a review of core processes. Annu Rev Psychol 58:259–289
66. Williams M (2014) Psychology and the art of trust maintenance. Paper presented at the 8th biennial workshop on trust within and between Organisations, Coventry UK, November 2014
67. Gioia DA, Chittipeddi K (1991) Sensemaking and sensegiving in strategic change initiation. Strateg Manag J 12(6):433–448
68. Lawrence T, Maitlis S (2014) The disruption of accounts: Sensebreaking in organizations. Working paper. Simon Fraser University
69. Vlaar PW, van Fenema PC, Tiwari V (2008) Cocreating understanding and value in distributed work: how members of onsite and offshore vendor teams give, make, demand, and break sense. MIS Q 32(2):227–255
70. Pratt MG (2000) The good, the bad, and the ambivalent: managing identification among Amway distributors. Adm Sci Q 45(3):456–493
71. Fox G, Tonge C, Mooney J, Lynn T (2018) Communicating compliance: developing and validating a GDPR privacy label. In: Proceedings of the the twenty fourth Americas conference on information systems, New Orleans, pp 16–18
72. Zorzo S, Pontes D, Mello J, Dias D (2016) Privacy rules: approach in the label or textual format. In: Proceedings of the twenty-second Americas conference on information systems, San Diego, pp 11–14
73. Lynn T, Van Der Werff L, Hunt G, Healy P (2016) Development of a cloud trust label: a Delphi approach. J Comput Inf Syst 56(3):185–193
74. Duranti L, Rogers C (2012) Trust in digital records: an increasingly cloudy legal area. Computer Law & Security Review 28(5):522–531
75. Podsakoff PM, MacKenzie SB, Lee JY, Podsakoff NP (2003) Common method biases in behavioral research: a critical review of the literature and recommended remedies. J Appl Psychol 88(5):879
76. McKnight DH, Carter M, Thatcher JB, Clay PF (2011) Trust in a specific technology: an investigation of its components and measures. ACM Transactions on Management Information Systems (TMIS) 2(2):12
77. Mayer RC, Gavin MB (2005) Trust in management and performance: who minds the shop while the employees watch the boss? Acad Manag J 48(5):874–888
78. Mayer RC, Davis JH (1999) The effect of the performance appraisal system on trust for management: a field quasi-experiment. J Appl Psychol 84(1):123
79. MacDonald AP Jr, Kessel VS, Fuller JB (1972) Self-disclosure and two kinds of trust. Psychol Rep 30(1):143–148
80. Söllner M, Leimeister JM (2010) Did they all get it wrong? Towards a better measurement model of trust. Paper Presented at the Academy of Management Annual Meeting, Montreal
81. McEvily B, Perrone V, Zaheer A (2003) Trust as an organizing principle. Organ Sci 14(1):91–103
82. Härting R-C, Moehring M, Schmidt R, Reichstein C, Keller B (2016) "What drives users to use CRM in a public cloud environment?-insights from European experts." in system sciences (HICSS), 2016 49th Hawaii international conference on, pp. 3999-4008. IEEE
83. Raman P, Wittmann CM, Rauseo NA (2006) Leveraging CRM for sales: the role of organizational capabilities in successful CRM implementation. J Pers Sell Sales Manag 26(1):39–53
84. Noor TH, Sheng QZ, Yao L, Dustdar S, Ngu AH (2016) CloudArmor: supporting reputation-based trust management for cloud services. IEEE transactions on parallel and distributed systems 27(2):367–380
85. ISO (2013) ISO/IEC 27000 family - information security management systems. https://www.iso.org/isoiec-27001-information-security.html. Accessed 25 Jan 2019
86. Emeakaroha VC, Fatema K, van der Werff L, Healy P, Lynn T, Morrison JP (2017) A trust label system for communicating trust in cloud services. IEEE Trans Serv Comput 10(5):689–700