Spring 5-15-2016

# TOWARDS A BRIGHT FUTURE: ENHANCING DIFFUSION OF CONTINUOUS CLOUD SERVICE AUDITING BY THIRD PARTIES

Sebastian Lins
*University of Cologne*, lins@wiso.uni-koeln.de

Heiner Teigeler
*University of Cologne*, teigeler@wiso.uni-koeln.de

Ali Sunyaev
*University Kassel*, sunyaev@uni-kassel.de

# TOWARDS A BRIGHT FUTURE: ENHANCING DIFFUSION OF CONTINUOUS CLOUD SERVICE AUDITING BY THIRD PARTIES

*Research*

Lins, Sebastian, University of Cologne, Cologne, Germany, lins@wiso.uni-koeln.de

Teigeler, Heiner, University of Cologne, Cologne, Germany, teigeler@wiso.uni-koeln.de

Sunyaev, Ali, University Kassel, Kassel, Germany, sunyaev@uni-kassel.de

## Abstract

*Using cloud services empowers organizations to achieve various financial and technical benefits. Nonetheless, customers are faced with a lack of control since they cede control over their IT resources to the cloud providers. Independent third party assessments have been recommended as good means to counteract this lack of control. However, current third party assessments fail to cope with an ever-changing cloud computing environment. We argue that continuous auditing by third parties (CATP) is required to assure continuously reliable and secure cloud services. Yet, continuous auditing has been applied mostly for internal purposes, and adoption of CATP remains lagging behind. Therefore, we examine the adoption process of CATP by building on the lenses of diffusion of innovations theory as well as conducting a scientific database search and various interviews with cloud service experts. Our findings reveal that relative advantages, a high degree of compatibility and observability of CATP would strongly enhance adoption, while a high complexity and a limited trialability might hamper diffusion. We contribute to practice and research by advancing the understanding of the CATP adoption process by providing a synthesis of relevant attributes that influence adoption rate. More importantly, we provide recommendations on how to enhance the adoption process.*

*Keywords: Cloud Computing, Continuous Auditing, Third Party Auditing, Diffusion of Innovations theory, Adoption*

# 1 Introduction

An increasing number of organizations outsource their data, applications, and business processes to the cloud, empowering them to achieve financial and technical benefits due to on-demand provisioning and pay-per-use pricing (Schneider and Sunyaev, 2016; Wolf and Rahn, 2015). Nonetheless, research shows that cloud services are facing a broad range of security issues, for instance, data breaches and losses as well as insecure interfaces (Cloud Security Alliance, 2015; Fernandes et al., 2014; Subashini and Kavitha, 2011). Likewise, media frequently discusses major cloud security flaws that remain undetected for a long time (e.g., iCloud's celebrity picture leakage (Arthur, 2014), and sensitive data breach of Epsilon's email clients (Schwartz, 2011)). With increasing reliance of organizations on cloud service providers to support their daily IT needs, the necessity for continuous, highly reliable, and secure services from a customer's perspective gains importance. Yet, customers are faced with a lack of governance and control since they necessarily cede control over their IT resources to the providers (Ackermann et al., 2011; European Network and Information Security Agency, 2009), and thus customers have to trust that providers fulfil demanded service levels and security requirements.

Extant research already proposes independent third party assessments and detective controls (i.e., auditing and certification) as good means to assess quality and performance of IT services in procurement processes to increase transparency and trust as well as to prove that providers fulfil demanded service levels (Khan and Malluhi, 2013; Sunyaev and Schneider, 2013; Pearson, 2011). These third party assessments are currently based on static, manual expert assessments and periodic spot checks only. In contrast, cloud computing environments are highly dynamic, resulting from challenging cloud computing characteristics (e.g., on-demand provisioning, entangled supply chains), fast technology life cycles, and ongoing architectural changes (Lins et al., 2016a; Bezzi et al., 2011). Likewise, cloud services are faced with dynamically emerging environmental challenges (e.g., new system vulnerabilities) as well as changes in legal and regulatory landscape. Current third party assessments fail to cope with this ever-changing environment due to static characteristics and long validity periods. Thus, we argue that continuous auditing by third parties (CATP) is required to deal with the ever-changing cloud environment, to assure continuously reliable and secure cloud services and to deal with customers' lack of control. Performing CATP is beneficial for cloud providers, auditors and customers altogether: Providers can improve their cloud systems by evaluating ongoing feedback about their performance; auditors actively detect and investigate critical auditing deviations as they occur, thus increasing auditing reliability; and finally CATP counteracts customers' lack of control by increasing the transparency of providers' operations (Lins et al., 2016a).

Past research has focused on implementing and evaluating continuous auditing (CA) of information systems since the late eighties. This progression has included the evolution of architecturally different methodologies, for instance, embedded audit modules (Groomer and Murthy, 1989) and independent monitoring control layers (Vasarhelyi and Halper, 1991), which help to continuously monitor and audit information systems. Yet, past research has mostly examined CA for internal purposes only. Just recently, various research projects and global organizations have started to deal with the development of innovative IT techniques and tools to enable third parties to continuously audit and assess cloud service behaviour. For example in the context of cloud computing, researchers recently proposed new means to enable independent third parties to audit data integrity (Wang et al., 2014) and to detect changes of cloud infrastructure (Doelitzscher et al., 2012) among others. Nonetheless, CATP remains currently underexplored, test marketed, and evaluated in trials only, resulting in a low adoption rate.

To predict and enhance CATP's rate of adoption, and therefore ultimately paving the way for continuously reliable and secure cloud services, we examine the diffusion and adoption process of CATP by building on the lenses of diffusion of innovations (DOI) theory (Rogers, 1962). Investigating how the attributes of an innovation affect its rate of adoption can be of great value to change agents seeking to predict and modify the reactions of their clients to an innovation (Rogers, 1962). When predicting an

innovation's rate of adoption is it more valuable to gather data on the attributes of the innovation prior to, or concurrently with, individuals' decisions to adopt the innovation (Rogers, 1962). We therefore conducted a scientific database search, and various focus group and one-to-one interviews with cloud service experts to gather and discuss data on the innovation's attributes that might enhance or hamper diffusion of CATP. Thereby answering the research questions: *RQ1: What influences the diffusion of CATP? RQ2: How can the CATP diffusion process be enhanced?*

Our findings reveal that perceived advantages, compatibility and observability of CATP would strongly enhance diffusion processes since CATP usage offers diverse advantages for each stakeholder, is compatible to existing sociocultural values and beliefs, and will be directly visible to the social system. In contrast, a high complexity and a limited trialability of CATP might hamper diffusion since CATP requires auditors and providers to make high initial IT infrastructure investments to participate. By analysing innovation's attributes that influence the diffusion of CATP and making recommendations to enhance diffusion processes, we contribute to practice and research in several ways. We advance the understanding of the CATP diffusion process by providing a synthesis and discussion of attributes that influence adoption rate from a DOI theory perspective. Further on, we guide future research as well as practitioners towards an adoption of CATP by providing recommendations on how to enhance the diffusion process, and to diminish adoption barriers.

The paper proceeds as follows. We provide a background on cloud computing, CA, and DOI theory, followed by a presentation of our research approach. In Section 4, we discuss how the attributes of CATP influence the diffusion process and make recommendations to enhance adoption. We then discuss consequences on the adoption rate in Section 5 and conclude with directions for future research.

# 2 Theoretical Background

## 2.1 Cloud Computing

Cloud Computing is a model that offers access to a shared pool of configurable IT resources (e.g., storage, platforms, and applications) that can be rapidly provisioned and released with minimal management effort (Mell and Grance, 2011). Cloud computing entails five essential characteristics that are the provision of (i) on-demand self-service access to (ii) virtualized, shared, and managed IT resources that are (iii) scalable on-demand, (iv) available over a network, and (v) priced on a pay-per-use basis. Cloud computing is facing many (new) security and privacy challenges, including but not limited to accessibility and virtualization vulnerabilities, physical access issues, and privacy and control issues (Fernandes et al., 2014; Subashini and Kavitha, 2011). To comply with federal and organizational compliance procedures and to prevent endangering their own business viability, cloud service customers demand a high level of security and reliability, and impose various requirements on cloud service operation. In order to fulfil these requirements, providers equip their data centres with sophisticated monitoring technologies and have set up internal auditing departments to quickly detect malicious behaviour, incidents, and service malfunctions (Aceto et al., 2013). However, monitoring and internal auditing of cloud infrastructures does not provide any proof to customers that the provided services are reliable and secure since relevant data is kept in-house to be solely inspected by system administrators and managers. To increase transparency, to address customers' concerns regarding security and reliability, and as to counteract customers' lack of control, cloud service providers have to prove credibility, for instance, by being continuously audited by independent auditors, and thereby informing users about up-to-date cloud system status (Lins et al., 2016b).

## 2.2 Continuous Auditing

Continuous auditing is defined as a methodology that enables independent auditors to provide written assurance on a subject matter, using a series of auditors' reports issued virtually simultaneously with,

or a short period of time after the occurrence of events underlying the subject matter (CICA/AICPA, 1999). Thus, CA enables auditors to react immediately to changes or events concerning the subject matter and to adjust their auditing reports based on assessment of these changes and events. In this study, we focus on continuous auditing by third parties since trusted third party intermediaries provide customers with genuine, independent and reliable information about cloud service operation. Moreover, they are considered to have some coercive power over the provider through promulgation and enforcement of explicit rules. Thus, a provider will make a sincere effort to uphold its transactional obligations (Kim, 2008; Zhang, 2005; Fukuyama, 1995).

Early works of Groomer and Murthy (1989) concerning implementation of embedded audit modules and Vasarhelyi and Halper (1991) regarding usage of monitoring and control layers spawned a research stream of CA. Therefrom, extant literature investigates implementation, transferability, and diffusion of CA in varying domains (Vasarhelyi et al., 2012; Brown et al., 2007; Woodroof and Searcy, 2001). Recently, researchers discussed CA of enterprise resource planning (ERP) systems (Singh et al., 2013; Kuhn Jr. and Sutton, 2010), accounting systems (Lin et al., 2010; Vasarhelyi et al., 2004), and web services (Yeh et al., 2008; Murthy and Groomer, 2004). However, past research has mostly examined CA for internal purposes only (Kiesow et al., 2015; Sun et al., 2015). In contrast to internal CA, CATP requires both—providers and auditors—to implement innovative information and communication technologies, including automated monitoring and auditing techniques, and more importantly, mechanisms for a secure exchange of audit-relevant information to continuously attest adherence to cloud requirements (Lins et al., 2016a; Lins et al., 2016b). A cloud service provider has to establish an internal monitoring and auditing department to perform extensive continuous monitoring and internal auditing operations to gather audit-relevant information. Therefrom, auditors request providers to transfer data and provide internal auditing reports according to defined frequencies. Besides, auditors can perform external CA to gather audit-relevant data, for example by deploying software agents on the cloud system to validate cloud infrastructure changes (Lins et al., 2015; Doelitzscher et al., 2012). Further on, auditing mechanisms and processes have to be implemented to automatically analyse audit-relevant data, to cope with identified deviations and to trigger alerts in cases of non-adherence.

Currently, various research projects have evolved, which deal with the development and evaluation of innovative techniques and tools to enable third parties to continuously audit and assess cloud service behaviour (e.g., NGCert (2015), and CUMULUS (2012)). Therefrom, different cutting-edge approaches to enable third party auditing are proposed in the context of cloud computing just recently, for example, methodologies to enable external auditors to simultaneously verify the integrity of multiple users' data (Wang et al., 2014) as well as architectures and metrics to support continuous validation of generic cloud (certification) requirements (Stephanow et al., 2016; Stephanow and Fallenbeck, 2015). Likewise, organizations such as Cloud Security Alliance and EuroCloud have just started to develop innovative processes and techniques for CATP of cloud services. Consequently, CATP currently remains underexplored, test marketed, and evaluated in trials only, and is therefore on its pre-diffusion stages (Rogers, 1983). We are examining the diffusion and adoption process of CATP by building on the lenses of DOI theory to predict and enhance future rate of adoption.

## 2.3 Diffusion of Innovations Theory

Diffusion of innovations theory is a well-known theory proposed by Rogers (1962) (Rogers, 2003; Rogers, 1983; Rogers and Shoemaker, 1971) and has been widely used for IT and information systems researches in recent decades (Larsen et al., 2015; Wu and Wang, 2005). DOI theory argues that potential users make decisions to adopt or reject an innovation based on beliefs they form about the innovation (Rogers, 2003). A central concept of the DOI theory is the diffusion process, in which an innovation is communicated through certain channels, over time, among the members of a social system. An innovation is any idea, object, or practice that is perceived as new by the members of a social system.

This theory has been applied in many different contexts (e.g., agriculture, marketing, IT, information systems) and to study a variety of innovations (e.g., spreadsheets, World Wide Web, EDI usage, software developing methods) (Larsen et al., 2015; Hardgrave et al., 2003; Iacovou et al., 1995). According to DOI theory, organizations can be classified into five adopter categories based on the point in time when they adopt the innovation relative to other organizations in their particular social system, namely innovators, early adopters, early majority, late majority, laggards (from earliest to latest adopters) (Beatty et al., 2001; Rogers, 1962). Further on, DOI theory describes five main innovation attributes that influence adoption rate of an innovation (Rogers, 1962). (1) Relative Advantage: The degree to which an innovation is seen as better than the idea, program, or product it replaces. (2) Compatibility: How consistent the innovation is with the values, experiences, and needs of the potential adopters. (3) Complexity: How difficult the innovation is to understand and/or use. (4) Trialability: The extent to which the innovation can be tested or experimented before adoption. (5) Observability: The extent to which the innovation provides tangible results. Because organizations adopt at different times, organizations in each of the adopter categories are believed to differ in their perceptions of attributes of the innovation. Rogers (1983) states that an innovation's relative advantage, compatibility, complexity, trialability, and observability were found to explain 49 to 87 percent of the variance in the rate of its adoption. Recent research findings confirm that these innovation attributes do explain acceptance behaviour in specific contexts, and that only complexity has a negative influence, while the other four attributes have a positive effect on facilitating the adoption of innovation (Hsu et al., 2007; Cheng et al., 2004; Chen et al., 2002; Agarwal and Prasad, 1997; Swanson and Ramiller, 1997).

Preceding influences have been demonstrated to underlie a variety of technology innovations in a wide variety of settings. Therefore, this theory provides a grounded framework that guides our exploration of factors that influence the CATP adoption process. Investigating how attributes of an innovation affect its rate of adoption can be of great value to change innovators seeking to predict the reactions of their potential users to an innovation, and perhaps to modify certain of these reactions by the way they name and position an innovation and relate the new idea to existing beliefs (Rogers, 1962). Therefore, we are investigating the adoption of CATP as an innovation in its pre-diffusion stages to predict and enhance the future rate of adoption.

# 3 Research Approach

By grounding our research on the DOI theory, we follow a deductive research approach and try to confirm that diffusion factors of DOI theory are prevalent and important in the context of CATP diffusion. We applied a two-step research approach. First, we conducted a scientific database search to identify relevant literature, and extract data on the innovation's attributes that might enhance or hamper diffusion of CATP. When predicting an innovation's rate of adoption is it more valuable to gather data on the attributes of the innovation prior to, or concurrently with, individuals' decisions to adopt the innovation (Rogers, 1962). Therefore, we conducted three workshops with cloud service providers, auditors, and consultants who are non-adopters of CATP, but are currently striving and participating in the innovative development of CATP as well as ten one-to-one interviews with cloud customers.

## 3.1 Literature Review

To gather data on the innovation's attributes, we performed a scientific database search in the following databases that cover a wide range of journals and conferences (i.e., they cover the top computer science and information systems journals and conferences): ACM Digital Library, AIS Electronic Library, EBSCOhost, Emerald Insight, IEEE Xplore, ProQuest and ScienceDirect. Each database was searched with the following search string in title and keywords: *(certif* OR audit* OR monitor* OR assur*) AND (continuous* OR permanent* OR dynamic* OR automat* OR real-time OR computerized OR (machine AND readable) OR (computer AND (assisted OR aided)))*. We filtered for peer-reviewed articles if possible and only considered articles that are published later than 1980 because the

concept of TCP/IP was introduced in 1981 (Postel, 1981). We identified 10,142 articles as potential relevant for our research. To make sure that these articles are relevant for our research, we analysed title, abstract, and keywords. Based on this relevancy check, we excluded 9,972 articles. We analysed the remaining 170 articles and validated the relevance of them in detail. We excluded 108 articles with research that does not deal with CA in particular, 13 articles that were not applicable to cloud computing contexts, and five that were non-research articles. Hence, we identified 44 articles as relevant for our research. Furthermore, a backward and forward analysis on the set of relevant articles was performed using Google Scholar (Webster and Watson, 2002). This backward search resulted in 1941 articles and the forward search yielded 2536 articles. Again, we made a relevancy validation, which led to additional twelve relevant articles. Finally, we read the remaining 66 articles extensively to gather data on the attributes of CATP. We identified various data concerning the innovation's relative advantages, complexity, and compatibility that helps us in discussing and predicting its adoption rate.

## 3.2 Cloud Expert Interviews

Identified literature mostly analyses the concept of CA in non-cloud contexts, for example accounting, ERP system, and web service contexts. To transfer and discuss literature review findings in the context of cloud computing, we conducted three focus groups and ten one-to-one interviews with cloud experts following the qualitative research method. Perhaps rather unusual for DOI literature, we choose a qualitative research approach to gather data since CATP is still on its pre-diffusion stage and therefore organizations that are familiar with the concept of CATP or even have adopted CATP are rare. Nonetheless, investigating how attributes of an innovation affect its rate of adoption can be of great value to enhance diffusion processes (Rogers, 2003). Conducting focus group interviews enable us to get collective views on a certain defined topic of interest from a group of people who are known to have had certain experiences (Myers, 2013). Furthermore, focus groups allow participants to engage in thoughtful discussions, hence generating practical oriented and rich data. We followed the recommendations by Myers (2013) and Donoghue (2000) to ensure that we perform our research approach rigorously. Therefore, four researchers carefully prepared and discussed interview guidelines beforehand, we followed a semi-structured interview approach to foster discussions among participants (Myers, 2013) and we used projective techniques to uncover the innermost thoughts and feelings of participants (Donoghue, 2000). During these focus group interviews, the concept of CATP was lively discussed and exemplarily transferred to individual use cases of practitioners. Focus group interviews were conducted in November and December 2014, and April 2015. In total, ten cloud service providers, nine cloud service auditors and five cloud service consultants participated. Each practitioner only participated in a focus group interview once. The cloud service providers are operating on a national and global scale, providing infrastructure, platform, and software business-to-business cloud services. Providers' sizes ranged from medium to large enterprises. Auditors have multi-year experience in conducting cloud service, infrastructure as well as data security and privacy audits. Further on, auditors are employed by large auditing or certification organizations, or work as independent auditors. Finally, participating consultants advise cloud customers when choosing cloud services as well as providers when deciding whether to get certified or not. Especially consultants were asked to represent a customer's perspective since no cloud service customer participated. Additionally, providers steadily reported on customer requests and opinions that they already experienced. Practitioners participated in our focus group interviews are non-adopters of CATP at the current research stage, but are currently striving and participating in the innovative development of CATP. This highly diverse setting of practitioners helped to gather data on the innovation's attributes that might enhance or hamper diffusion. A focus group interview lasted on average 4 hours and 30 minutes and all three focus group interviews lasted 15 hours in total. Since no cloud customer participated in focus group interview, we performed ten semi-structured one-to-one interviews with cloud service customers. One-to-one interviews allow gathering of rich data from people in different roles (Myers, 2013). Furthermore, semi-structured interviews involve use of pre-formulated questions but allow improvisation for emerging topics during conversation. Inter-

viewees are IT managers from medium to large enterprises and different sectors, including IT, health, trade, and finance. Interview guidelines were derived and discussed by three researchers beforehand. An interview lasted on average 60 minutes. Interviews were conducted between June and July 2015, and no cloud customer was interviewed twice.

The focus group interviews and one-to-one interviews were recorded, transcribed, and analysed by three researchers independently, applying qualitative data coding techniques (Myers, 2013) (software used: ATLAS.ti 7). We followed a two stage coding approach: first performing open coding, and second axial coding. Our initial stage of analysis (open coding) aimed at identifying data that describes the innovation's attributes, and more importantly to derive corresponding recommendations from practitioners. On the second stage of analysis (axial coding), we used the five innovation attributes from DOI theory as well as findings from the literature review to evaluate and confirm that these are accurately represented by interview responses. Finally, based up insights gained during this coding analyses we were able to gather various data concerning the innovation's relative advantages, complexity, compatibility, and observability that supports us in discussing and predicting adoption rate. More importantly, we were able to derive recommendations to enhance future diffusion of CATP. We discuss interview findings and recommendations in Section 4, and highlight our qualitative findings by citing corresponding stakeholders in brackets.

# 4 Adoption of Continuous Auditing by Third Parties

## 4.1 Relative Advantage

When organizations pass through the innovation-decision process, they are motivated to seek information in order to decrease uncertainty about the relative advantage of an innovation (Rogers, 1983). Relative advantages refers to the degree to which an innovation is perceived as being better than its precursors (i.e., resolving existing problems, or savings in time and effort) (Rogers, 1983). For CATP of cloud services to become widely adopted, it must be technologically and economically feasible. Providers as well as auditors must be motivated and have the expertise to participate. To motivate them, perceived advantages must be higher than perceived expenditures. Therefrom, we will highlight and discuss great advantages for auditors, service providers and cloud customers to foster adoption.

Cloud service providers can take various advantages by participating in CATP. First, practitioners emphasize that CATP improves service and risk management of providers (Provider). Implementing suitable continuous monitoring and internal CA techniques, and evaluating continuous feedback about how cloud services are performing improves quality of internal processes and systems (Kott and Arnold, 2013; National Institute of Standards and Technology, 2011; Alles et al., 2006; Provider). In addition, providers receive ongoing third party expert assessments about their systems. Therefrom, providers are able to detect potential flaws and (security) incidents earlier and can save costs due to successive service improvements. Further on, improvements and enhancements of cloud infrastructure, software, or processes (e.g., due to agile development)—after the initial certification—can be considered earlier and reflected in the certification report due to ongoing assessment (Provider; Auditor). Interviewed service providers report that they are occasionally confronted with business customers' requests for individual customer audits due to intransparent cloud services and concerns regarding cloud service security. These individual customer audits burden high expenses and efforts for providers. Practitioners assume that participating in CATP will reduce the need for individual customer audits since genuine auditing results will be provided to customers by an independent party, thereby increasing result trustworthiness and ultimately leading to additional cost savings for providers (Provider). When participating in CATP, providers might offer value added customer services to reuse data that is gathered for CA purposes, for example, special monitoring services, specification of individual monitoring thresholds and corresponding alert newsletters as well as an interactive web frontend for enhanced customer support (Customer; Provider). Finally, providers can differentiate themselves in

the cloud market by making their cloud services more transparent, accountable, and approachable for customers (Auditor; Customer; Provider). Thus, cloud service providers may gain competitive advantages in participating in CATP.

Auditors can improve audit efficiency by reducing auditing time and errors due to automated auditing processes (Shin et al., 2013; Alles et al., 2006; Woodroof and Searcy, 2001; Auditor). Likewise, CA is more cost-effective by enabling auditors to test larger samples and examine data faster and more efficiently compared to their manual predecessors (Brown et al., 2007; Rezaee et al., 2002; Woodroof and Searcy, 2001; Auditor). Auditors can counteract lack of cloud customers' control in cloud environments by increasing transparency regarding operations of service providers (Auditor; Customer). Typically, adherence to certification criteria is observed by spot checks on a yearly basis. Hence, certification deviations or breaches might be detected lately. In contrast, CA allows auditors to actively detect and investigate exceptions as they occur rather than to react after exceptions have long occurred (Chiu et al., 2014; Chan and Vasarhelyi, 2011; Flowerday et al., 2006; Auditor; Customer). Hence, CA can be considered as proactive and enables corrective action to be taken as soon as a problem is detected. More importantly, through timely detection and continuous assurance of certification adherence, CATP can improve trustworthiness and perceived assurance of auditors' certifications (Auditor; Customer). Further on, reports of auditors are more relevant to decision makers of potential cloud service adopters due to timely and up-to-date information with regard to certified criteria (Woodroof and Searcy, 2001; Auditor; Customer). Similar to cloud service providers, auditors might offer new value added services for cloud customers, thus enabling new auditing business models (Auditor). For example, auditors can provide cloud customers with on-demand auditing capabilities (e.g., triggering auditing operations), periodic audit reports, and alerting services (e.g., on major security incidents or certification violations) among others that require customers to pay a usage fee.

To achieve aforementioned provider and auditor advantages and thereby enhancing diffusion of CATP, practitioners recommend developing and implementing mostly standardized and interoperable CATP practices and systems (Auditor; Provider). First, providers can benefit when using flexible and interoperable CATP structures and processes by reducing auditor dependency, potential sunk, and switching costs, and hence preventing auditor lock-in effects. Second, auditors are faced with a high individualism and complexity of an auditee's cloud service systems, resulting from customized or legacy systems as well as incorporated third party services. Implementing flexible and standardized CATP systems allows them to easily integrate or exclude providers since they might concurrently audit a broad variety of different cloud service providers. Moreover, a precise distinction between providers' continuous monitoring and CATP operations and responsibilities is recommended (Auditor). Performing continuous monitoring by a provider forms a prerequisite for auditors to perform efficient CATP. However, it has to be ensured that providers do not outsource their entire monitoring and assessment processes to third party auditors. For instance, CA of system vulnerabilities on a monthly basis might be viewed as a substitute for internal vulnerability management by a provider. Consequently, practitioners recommend that an auditor gathers the results of vulnerability analysis from providers on a monthly basis and assesses certification adherence on a quarterly or semi-annually basis in the context of vulnerability management in this exemplarily case.

According to DOI theory, incentives may be paid either directly to an adopter, or to another individual to encourage him or her to persuade an adopter (Rogers, 1983). Thus, especially if an increasing amount of customers demand trustworthy (certified) cloud services, providers may start to open up for CATP. In general, cloud service customers can benefit when CATP is performed as well. Typically, cloud environments are characterized by a lack of control since cloud customers cedes governance to cloud service providers (European Network and Information Security Agency, 2009). CATP can counteract this lack of control by increasing transparency regarding operations of providers, and providing assurance regarding requirements (e.g., ensuring encryption, data integrity, and location)—ultimately enhancing trustworthiness of customers in cloud services (Auditor; Customer; Provider). Finally, audit findings might be used as evidence in courts, thereby CATP can give sufficient legal grounds for a

lawsuit, supporting small or mid-sized customers' organization in legal conflicts with providers (e.g., in cases providers void service level agreements or major security incidents appear) (Customer).

Yet, interviewed customers emphasized that preventing cloud service providers to manipulate or euphemize audit-relevant data is an important prerequisite for CATP diffusion and to ensure that CATP is trustworthy and reliable since most audit-relevant data will be provisioned by a provider herself. Therefore, providers and auditors should build on findings from research area of cloud forensics that deals with the application of scientific principles, technological practices, and proven methods to reconstruct past cloud computing events through identification, collection, preservation, examination, interpretation, and reporting of digital evidence (National Institute of Standards and Technology, 2014). Researchers have proposed various procedures (e.g., chain of custody (Lin et al., 2012); trusted third party modules (Pichan et al., 2015); homomorphic encryption (Rajalakshmi et al., 2014)) to deal with malicious cloud service providers manipulating data, ultimately enabling third party investigators to collect and analyse reliable, trustworthy, and accountable data (Pichan et al., 2015).

## 4.2 Compatibility

A high innovation's compatibility enhances the diffusion of an innovation since an innovation that is more compatible is less uncertain to the potential adopter (Rogers, 2003). Compatibility is the degree to which an innovation is perceived as consistent with (1) the existing sociocultural values and beliefs, (2) previously introduced ideas, and (3) needs of potential adopters.

Certifications, web assurance structures and quality seals are established and well-recognised means for customers and organizations to assess goods and services (Sturm et al., 2014; Khan and Malluhi, 2010; Praeg and Schnabel, 2006). Importance and number of independent third party product and service assessments steadily increase in recent years (International Organization for Standardization, 2014). For example, the information security standard ISO/IEC 27001 shows a growth rate of 7% in 2014 compared to 2013, resulting in more than 23,000 certified organizations worldwide. More importantly, the European Union has declared the development and diffusion of cloud certifications as a major action when fulfilling their strategy for 'Unleashing the Potential of Cloud Computing in Europe' (European Commission, 2012). Hence, current cloud service providers, customers, and auditors believe in and demand third party assessments. Similar, organizations and research have focused on implementing and evaluating internal CA of information systems since the late eighties. For these reasons, it can be assumed that the innovation of CATP is consistent with current sociocultural values and beliefs, and therefore organizations are more likely to adopt this innovation. Yet, past research has mostly examined CA for internal purposes only, thus we recommend that organizations and researchers have to transfer and broaden internal CA concepts to third party contexts by implementing innovative information and communication technologies, including continuous monitoring and auditing systems, allocate corresponding responsibilities, and more importantly, to root continuous third party expert assessments into their organizational strategy and orientation.

Previous introduced ideas and practice are a familiar standard against which the innovation can be interpreted, thus decreasing uncertainty (Rogers, 2003). Current third party auditing practices are mostly based upon manual auditing operations, for example, performing interviews and manual security tests as well as analysing service and architecture documentations (Auditor). Automation of these current auditing processes increases audit efficiency by enabling auditors to test larger samples and examine data in a faster way (Woodroof and Searcy, 2001; Auditor). Subsequently, researchers and major accounting organizations have already developed various computer-assisted auditing tools and technologies (CAATT) since the 1980s (Ahmi and Kent, 2012; Chou et al., 2007). These tools comprise, for example, generalized auditing software, electronic working papers, tools for fraud detection, and just recently CA functions, and can be used to connect to an auditee's information system, automatically extract, sample, and analyse audit-relevant data (ACL Services Ltd., 2015; Mahzan and Lymer, 2014; Pedrosa and Costa, 2014). The previous introduction of CAATT can be seen as facilita-

tor for diffusion of CATP since CAATT aim to automate processes and support auditors in performing (continuous) assessments. Yet, research suggests that auditors do not frequently and systematically use CAATT during their auditing processes despite various emphasizes on CAATT usage and potential advantages (Abou-El-Sood et al., 2015; Bierstaker et al., 2014; Mahzan and Lymer, 2014). Likewise, research suggests that an automation and computerization of auditing processes is likely to be incremental rather than disruptive since auditors will likely attempt to first automate existing processes rather than developing technology enabled auditing processes (Alles et al., 2006; Alles et al., ). Consequently, we recommend that practitioners and future research should analyse existing research findings on CAATT adoption, and learn from (failures of) CAATT diffusion processes to enhance the diffusion of CATP. For example, research on CAATT suggests that auditors' employees should attend comprehensive trainings to counteract a low confidence in their technical abilities or a lack of knowledge (Vasarhelyi et al., 2012), and be encouraged through positive reviewer comments, bonuses, and promotion criteria to enhance diffusion processes (Bierstaker et al., 2014).

Another indication of the compatibility of an innovation is the degree to which it meets a need felt by the clients (Rogers, 2003). When felt client needs are met by an innovation, a faster rate of adoption usually occurs. Interviews with cloud experts revealed a strong need for CATP. First, interviewees reported that for many customers using the cloud is comparable to sending data into a black box, losing control over their data, and retrieving cloudy results (Customer; Provider). Consequently, customers demand performing CATP to counteract these issues, and to prove adherence to relevant certification, or legal requirements. Second, providers aim to gain competitive advantages due to transparent cloud services (Provider). Finally, auditors are willing to participate in CATP to counteract drawbacks of traditional certifications, which only represent a retrospective look at the fulfilment of measures at the time of their issuing (Auditor). Such needs probably will accelerate diffusion of CATP.

## 4.3 Complexity

Complexity is the degree to which an innovation is perceived as relatively difficult to understand and use (Rogers, 1962). The introduction of a new technology typically requires the organization to integrate (expensive) hard- and software into its existing IT infrastructure, and can be intimidating for organizational employees, particularly if it requires them to change their existing business practices or acquire new skills (Beatty et al., 2001; Rogers, 1983). Therefore, a consistent finding from the technology diffusion literature is that technological complexity is a significant factor inhibiting implementation and adoption success (Bradford and Florin, 2003; Tornatzky and Klein, 1982).

Performing CATP inherits a high degree of complexity since it requires providers and auditors to set up comprehensive monitoring and auditing infrastructures (Auditor; Provider). Providers need to implement large-scale (continuous) monitoring systems to ensure that all audit-relevant data is available, up-to-date, and accurate. Continuous monitoring operations should at least comprise gathering data by monitoring of physical resources and virtualized environments, security and privacy monitoring as well as service level monitoring. In addition to performing extensive monitoring processes, a provider might implement internal (continuous) auditing systems to gather audit-relevant data across different monitoring systems, to aggregate (monitoring) data and format data according to auditors' needs. According to DOI theory, the more compatible an innovation is with existing systems, the greater the chances of realizing organizational benefits (Rogers, 2003; Tornatzky and Klein, 1982), and the more satisfied users will be (DeLone and McLean, 1992). Thus, we recommend to leverage existing cloud monitoring systems for CATP purposes since providers have already equipped their service centres with sophisticated monitoring technologies to gather service data (Aceto et al., 2013). However, traditional monitoring systems are designed for internal monitoring purposes only, and the gathered monitoring information is kept in-house to be solely inspected by system administrators. Consequently, current monitoring systems are lacking a proper threat model and respective functionality to integrate external auditors, and present monitored information in an aggregated and anonymized fashion to cus-

tomers without revealing confidential information on the cloud infrastructures. Future research need to analyse how existing monitoring systems can be leveraged for CATP purposes. Likewise, auditors need to implement continuous auditing systems, comprising various auditing methods to perform (semi-)automated and external auditing processes. Hence, for example, performing penetration testing, external vulnerability scans, and using interceptor tools to analyse cloud systems, service availability, and encryption (Lins et al., 2016a). Moreover, auditors have to implement systems to support audit planning, management and scheduling to coordinate CATP processes and to enable fluent and automated execution of auditing functions. We recommend that practitioners and researchers should focus on developing new efficient CATP architecture (cf. Lins et al., 2016b; Stephanow et al. (2016)) since currently most CA methodologies are developed for internal contexts.

Decreasing system complexity and ensuring economic feasibility is of critical importance when designing and performing CATP (Auditor; Provider). Thus, an adequate and individual auditing scope has to be defined based upon the cloud service and auditee's context, for example, considering the extent of implemented cloud systems, offered service functions, size of the auditee's enterprise, as well as the auditees' level of technical knowledge and skills (Auditor). Nonetheless, future auditing systems should be maintainable (e.g., administrating existing modules), reliable (e.g., low performance impacts and high availability), and adaptable (e.g., updating and adjusting modules to changes) (Lin et al., 2010; Alles et al., 2006) to cope with the ever-changing environment of cloud services.

Besides setting up comprehensive monitoring and auditing infrastructures, providers and auditors are faced with new security challenges in the context of CATP, which in turn increase complexity of using this innovation. Assuring confidentiality (e.g., preventing leakage of sensitive or security-relevant information), availability (e.g., ensuring availability of data exchange interfaces), and integrity (e.g., guarding information against malicious modification by attackers, auditors or providers) is of critical importance when designing continuous auditing processes and systems (Auditor; Customer; Provider). Especially the exchange of audit-relevant information through using (web) interfaces requires providers and auditors to implement secure access control systems as well as encryption mechanisms to prevent data leakage during data transmission. Consequently, future research and practitioners should identify, evaluate, and provide the means to diminish potential risks and threats for auditees' and auditors' operating systems.

## 4.4 Trialability and Observability

Trialability is the degree to which an innovation may be experimented before adoption (Rogers, 1983). Innovations that can be tried in advance will generally be adopted more rapidly than innovations that are not divisible. CATP does not possess a high degree of trialability since it exhibits a high degree of complexity, and providers as well as auditors have to invest high initial expenditures to participate on the current pre-diffusion and innovator stage (Auditor; Provider). Nonetheless, we recommend auditors to offer online demos that simulate a free trial of a (fictional) continuous cloud service audit, and to offer interface mock-ups as well as auditee's success stories to substitute limited trialability capabilities. Thereby, these substitutes might enhance diffusion processes.

In contrast to trialability, performing CATP achieves high degree of observability. Observability is the degree to which the results of an innovation are visible to others, and is positively related to its rate of adoption (Rogers, 1983). The results of some innovations are easily observed and communicated to members of a social system, whereas some innovations are difficult to describe to others. Interviewees put high emphasize on cloud customer enlightenment when performing CATP to counteract customers' fear of loss of control and to counteract the impression of using a black box when provisioning cloud services (Auditor; Customer; Provider). To foster observability, it is therefore of critical importance to publish auditing information on a continuous basis to prove ongoing adherence to audit requirements. In addition, practitioners recommend presenting comprehensive information about cloud service performance to prove ongoing customer, legal and regulatory requirement adherence, ultimate-

ly increasing the transparency about cloud services (Customer; Provider). Therefrom, performing continuous auditing provides customers with insights that might go beyond what they can analyse themselves or what is offered by the providers since auditors possess required knowledge and technical expertise, and might have more access to sensitive data. Further on to increase comprehensibility and accountability of CATP—and thereby enhancing its observability—practitioners recommend informing customers about how and when data was gathered and analysed (Customer). More importantly, in cases of critical requirement violations or major (security) incidents, customers should be automatically informed by auditors (Customer). Subsequently, we recommend that a user interface (e.g., a web frontend for customers) to inform customers about continuous auditing processes, corresponding results, and general cloud service operation is required to foster observability of this innovation. Such a customer frontend can be used as a communication platform between providers and customers as well, in which for example, security incidents are posted and updated when solved, thus reducing customer support inquiries (Provider). Similar, performing CATP offers the means for a new generation of web assurance seals: dynamic, up-to-date, and accurate seals informing customers about the actual requirement adherence status and the point in time of the last validity assessment. Nonetheless, achieving a high degree of observability requires providers and auditors to aggregate, and anonymize monitoring and auditing data to cope with data confidentiality, integrity, and authenticity challenges.

# 5 Discussion

According to DOI theory, the preceding five main innovation attributes highly influence adoption rate of an innovation (Rogers, 1983). By reviewing literature on CA and conducting manifold interviews with cloud experts, we have evaluated and shown that these attributes are relevant for the diffusion of CATP. Consistent with literature on diffusion processes (Hsu et al., 2007; Cheng et al., 2004; Swanson and Ramiller, 1997; Rogers, 1983), we believe that the multifarious relative advantages of CATP will strongly motivate providers and auditors to adopt the auditing innovation, and might be the most important predictor of adoption rate. In this regard, a high degree of compatibility to existing sociocultural values and beliefs, the diffusion facilitation due to previously introduced CAATT, and a high need of relevant stakeholders will further accelerate the diffusion process. Observability might be even more a crucial factor influencing adoption rate than compatibility since the primary objective of CATP is to increase transparency about cloud services, and therefore innovation usage will be immediately visible to the social system. Still, a high degree of complexity and limited trialability caused by high initial investments will strongly hamper innovation adoption at early diffusion stages.

Other factors might influence adoption rate, besides the innovation's attributes. Market forces are of importance in explaining the rate of adoption of innovations (Rogers, 1983). Thus, market forces like competitive pressure and imposition by supply chain partners might influence future CATP adoption. The need to develop and sustain a competitive advantage in the marketplace is what drives successful business strategies (Porter, 2004). Either the incentive of first mover competitive advantages or the urgency to keep up with competitors will provide the focus and purpose to successfully overcome obstacles and resistance to innovation adoption within an organization (Bradford and Florin, 2003; Iacovou et al., 1995; Zaltman et al., 1973). Hence, as more competitors become capable of participating in CATP, other organizations might be more inclined to adopt CATP in order to maintain their own competitive position. Likewise, innovation imposition strategies by supply chain partners might foster adoption rate of CATP, for example, by recommending or rewarding participation in CATP, or by threatening organizations (e.g., applying negative sanctions) (Iacovou et al., 1995), especially since provisioned cloud services are often part of entangled supply chains (Cimato et al., 2013).

DOI theory proposes that there will be different adopter groups over innovation diffusion stages (see Section 2.3). Because organizations adopt at different times, organizations in each of the adopter categories differ in their perceptions of attributes of the innovation and their perception of the innovations attributes may change as the innovation diffuses (Rogers, 1983). In case of CATP diffusion, relative

advantages might be less important in later diffusion stages since CATP might become best practice or standard for cloud service provisioning. Thus, instead of focusing on achieving innovation's advantages, competitive pressure might require providers to participate in CATP in the future. More importantly, future development of standardized and flexible auditing systems, and establishment of best practices in third party auditing will diminish the high degree of complexity as CATP diffuses. Similar, monitoring and auditing tool vendors might start to implement standardized interfaces to enable easy data extraction for CATP purposes, thus fostering trialability capabilities of the innovation.

# 6 Conclusion

*"Last, […] an innovation's rate of adoption is affected by the extent of change agents' promotion efforts"* (Rogers, 1983, p. 234-234). On this account, we want to encourage researchers and practitioners with this study to participate in developing and diffusing CATP by discussing innovation's attributes that influence adoption rate and making recommendations to enhance diffusion processes based on findings from reviewing literature on CA and performing interviews with cloud experts. We believe that CATP of cloud services is one possible way to address current gaps and issues in ever-changing cloud environment, ultimately creating more trustworthy and transparent cloud services.

Findings from our work indicate that on the one hand, especially relative advantages and observability will enhance CATP adoption, and on the other hand, a high degree of complexity might hamper diffusion processes. Thereby, we provide a two-fold contribution for research and practice. We advance the understanding of the CATP diffusion process by providing a synthesis and discussion of relevant factors that influence adoption rate from a DOI theory perspective. Investigating how the attributes of an innovation affect its rate of adoption can be of great value to change agents seeking to predict the reactions of their clients to an innovation, and perhaps to modify certain of these reactions by the way they name and position an innovation (Rogers, 1962). Finally, we guide future research as well as practitioners towards an adoption of CATP by providing recommendations on how to enhance the diffusion process, and to diminish adoption barriers.

Nevertheless, this study has some limitations. Our discussion of the diffusion process is based on literature analysis and qualitative research only since at the current diffusion state a minority of cloud providers and auditors have started to deal with CATP adoption. Thus, quantitative studies have to be conducted on later diffusion stages (i.e., number of adopters reaches the minimum for reliable quantitative results) to analyse to what extent the discussed attributes of an innovation influence its diffusion. In addition, our qualitative data might be slightly biased to some degree since we interviewed cloud providers, auditors and consultants who may have a financial interest in CATP development and diffusion. Likewise, measuring the perceived attributes of an innovation at the current diffusion stage provides only a limited picture of the relationship of such attributes to an innovation's rate of adoption since the characteristics may change as the innovation diffuses (Rogers, 1983).

Our results pave the way for several future research avenues. First, further research should focus on developing auditing methodologies adjusted to the CATP context, especially concerning validation of security measures and adherence to critical cloud service characteristics (e.g., availability and scalability of services). Second, research should focus on how to decrease innovation's complexity to enhance adoption rate (e.g., by designing interoperable systems and leveraging providers' existing monitoring capabilities). Finally, future research should clarify how to manage requirement violations and how to inform customers about requirement (non-)adherence to address current concerns of customers.

# 7 Acknowledgements

This research is funded by the German Federal Ministry for Education and Research (grant no. 16KIS0079). We thank the associate editor and three anonymous reviewers for their constructive feedback, which helped us to improve the manuscript.

## References


Abou-El-Sood, H., Kotb, A. and A. Allam (2015). Exploring Auditors' Perceptions of the Usage and Importance of Audit Information Technology. *International Journal of Auditing,* 19 (3), 252–266.

Aceto, G., Botta, A., Donato, W.d. and A. Pescapè (2013). Cloud monitoring: A survey. *Computer Networks,* 57 (9), 2093–2115.

Ackermann, T., Miede, A., Buxmann, P. and R. Steinmetz (2011). "Taxonomy of Technological IT Outsourcing Risks: Support for Risk Identification and Quantification." In: *Proceedings of the 19th European Conference on Information Systems,* 1–16.

ACL Services Ltd. (2015). *ACL Solutions.* URL: www.acl.com/solutions/products (visited on 04. Apr 2016).

Agarwal, R. and J. Prasad (1997). The Role of Innovation Characteristics and Perceived Voluntariness in the Acceptance of Information Technologies. *Decision Sciences,* 28 (3), 557–582.

Ahmi, A. and S. Kent (2012). The utilisation of generalized audit software by external auditors. *Managerial Auditing Journal,* 28 (2), 88–113.

Alles, M., Kogan, A., Brennan, G. and M. A. Vasarhelyi (2006). Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens. *International Journal of Accounting Information Systems,* 7 (2), 137–161.

Alles, M.G., Kogan, A. and M. A. Vasarhelyi (). Audit automation for implementing continuous auditing.

Arthur (2014). *Nude celebrity picture leak looks like phishing or email account hack.* URL: www.theguardian.com/technology/2014/sep/01/nude-celebrity-pictures-hack-jennifer-lawrence-rihanna (visited on 04. Apr 2016).

Beatty, R.C., Shim, J. and M. C. Jones (2001). Factors influencing corporate web site adoption: a time-based assessment. *Information & Management,* 38 (6), 337–354.

Bezzi, M., Kaluvuri, S.P. and A. Sabetta (2011). "Ensuring trust in service consumption through security certification." In: *Proceedings of the International Workshop on Quality Assurance for Service-Based Applications,* 40–43.

Bierstaker, J., Janvrin, D. and Lowe, D. Jordan (2014). What factors influence auditors' use of computer-assisted audit techniques? *Advances in Accounting,* 30 (1), 67–74.

Bradford, M. and J. Florin (2003). Examining the role of innovation diffusion factors on the implementation success of enterprise resource planning systems. *International Journal of Accounting Information Systems,* 4 (3), 205–225.

Brown, C.E., Wong, J.A. and A. A. Baldwin (2007). A review and analysis of the existing research streams in continuous auditing. *Journal of Emerging Technologies in Accounting,* 4 (1), 1–28.

Chan, D.Y. and M. A. Vasarhelyi (2011). Innovation and practice of continuous auditing. *International Journal of Accounting Information Systems,* 12 (2), 152–160.

Cheng, J.M.S., Kao, L.L.Y. and J. Y.-C. Lin (2004). An Investigation of the Diffusion of Online Games in Taiwan: An Application of Roger's Diffusion of Innovation Theory. *Journal of American Academy of Business,* 5 (1/2), 439–445.

Chen, L.-d., Gillenson, M.L. and D. L. Sherrell (2002). Enticing online consumers: an extended technology acceptance perspective. *Information & Management,* 39 (8), 705–719.

Chiu, V., Liu, Q. and M. A. Vasarhelyi (2014). The development and intellectual structure of continuous auditing research. *Journal of Accounting Literature,* 33 (1–2), 37–57.

Chou, C.L.-y., Du, T. and V. S. Lai (2007). Continuous auditing with a multi-agent system. *Decision Support Systems,* 42 (4), 2274–2292.

CICA/AICPA (1999). Continuous auditing, The Canadian Institute of Chartered, Toronto, Canada.

Cimato, S., Damiani, E., Menicocci, R. and F. Zavatarelli (2013). "Towards the certification of cloud services." In: *IEEE Ninth World Congress on Services (SERVICES),* 100–105.

Cloud Security Alliance (2015). *Cloud Adoption Practices & Priorities Survey Report.* URL: downloads.cloudsecurityalliance.org/initiatives/surveys/capp/Cloud_Adoption_Practices_Priorities_Survey_Final.pdf (visited on 04. Apr 2016).

CUMULUS (2012). *Certification infrastructure for multi-layer cloud services.* URL: www.cumulus-project.eu (visited on 04. Apr 2016).

DeLone, W.H. and E. R. McLean (1992). Information Systems Success: The Quest for the Dependent Variable. *Information Systems Research,* 3 (1), 60–95.

Doelitzscher, F., Fischer, C., Moskal, D. and C. Reich, et al. (2012). "Validating cloud infrastructure changes by cloud audits." In: *IEEE Eighth World Congress on Services (SERVICES),* 377–384.

Donoghue, S. (2000). Projective techniques in consumer research. *Journal of Family Ecology and Consumer Sciences,* 28.

European Commission (2012). *Unleashing the Potential of Cloud Computing in Europe.* URL: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF (visited on 25. Nov 2015).

European Network and Information Security Agency (2009). *Cloud Computing.* URL: www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment (visited on 13. Nov 2015).

Fernandes, D.A.B., Soares, L.F.B., Gomes, J.V., Freire, M.M. and P. R. M. Inácio (2014). Security issues in cloud environments: a survey. *International Journal of Information Security,* 13 (2), 113–170.

Flowerday, S., Blundell, A.W. and R. von Solms (2006). Continuous auditing technologies and models: A discussion. *Computers & Security,* 25 (5), 325–331.

Fukuyama, F. (1995). *Trust.* Free Press, New York.

Groomer, S.M. and U. S. Murthy (1989). Continuous auditing of database applications. *Journal of Information Systems,* 3 (2), 53–69.

Hardgrave, B.C., Davis, F.D. and C. K. Riemenschneider (2003). Investigating Determinants of Software Developers' Intentions to Follow Methodologies. *Journal of Management Information Systems,* 20 (1), 123–151.

Hsu, C.-L., Lu, H.-P. and H.-H. Hsu (2007). Adoption of the mobile Internet: An empirical study of multimedia message service (MMS). *Special Issue on Telecommunications Applications,* 35 (6), 715–726.

Iacovou, C.L., Benbasat, I. and A. S. Dexter (1995). Electronic Data Interchange and Small Organizations: Adoption and Impact of Technology. *Management Information Systems Quarterly,* 19 (4), 465–485.

International Organization for Standardization (2014). *The ISO Survey of Management System Standard Certifications – 2014.* URL: www.iso.org/iso/iso-survey (visited on 23. Nov 2015).

Khan, K. and Q. Malluhi (2010). Establishing trust in cloud computing. *IT Professional,* 12 (5), 20–27.

Khan, K.M. and Q. Malluhi (2013). Trust in Cloud Services: Providing More Controls to Clients. *Computer,* 46 (7), 94–96.

Kiesow, A., Zarvic, N. and O. Thomas (2015). "Improving the Success of Continuous Auditing Projects with a Comprehensive Implementation Framework." In: *Proceedings of the 23rd European Conference on Information Systems,* 1–16.

Kim, D.J. (2008). Self-Perception-Based Versus Transference-Based Trust Determinants in Computer-Mediated Transactions: A Cross-Cultural Comparison Study. *Journal of Management Information Systems,* 24 (4), 13–45.

Kott, A. and C. Arnold (2013). The Promises and Challenges of Continuous Monitoring and Risk Scoring. *IEEE Security & Privacy,* 11 (1), 90–93.

Kuhn Jr., J.R. and S. G. Sutton (2010). Continuous auditing in ERP system environments. *Journal of Information Systems,* 24 (1), 91–112.

Larsen et al. (2015). *Theories Used in IS Research Wiki.* URL: is.theorizeit.org (visited on 04. Apr 2016).

Lin, C.-C., Lin, F. and D. Liang (2010). "An analysis of using state of the art technologies to implement real-time continuous assurance." In: *2010 6th World Congress on Services (SERVICES)*, 415–422.

Lin, C.-H., Lee, C.-Y. and T.-W. Wu (2012). A Cloud-aided RSA Signature Scheme for Sealing and Storing the Digital Evidences in Computer Forensics. *International Journal of Security and Its Applications*, 6 (2), 241–244.

Lins, S., Thiebes, S., Schneider, S. and A. Sunyaev (2015). "What is Really Going on at Your Cloud Service Provider?" In: *Hawaii International Conference on System Sciences*, Kauai, Hawaii, USA, 1–10.

Lins, S., Grochol, P., Schneider, S. and A. Sunyaev (2016a). Dynamic Certification of Cloud Services. *IEEE Security & Privacy*, 14 (2),

Lins, S., Schneider, S. and A. Sunyaev (2016b). Trust is Good, Control is Better: Creating Secure Clouds by Continuous Auditing. *IEEE Transactions on Cloud Computing*, in Press.

Mahzan, N. and A. Lymer (2014). Examining the adoption of computer-assisted audit tools and techniques. *Managerial Auditing Journal*, 29 (4), 327–349.

Mell, P. and T. Grance (2011). The NIST definition of cloud computing, Gaithersburg and Montgomery and USA.

Murthy, U.S. and S. Michael Groomer (2004). A continuous auditing web services model for XML-based accounting systems. *International Journal of Accounting Information Systems*, 5 (2), 1–31.

Myers, M.D. (2013). *Qualitative research in business & management.* 2nd Edition. SAGE, London.

National Institute of Standards and Technology (2014). NIST Cloud Computing Forensic Science Challenges: Draft NISTIR 8006.

National Institute of Standards and Technology (2011). *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.* URL: csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf (visited on 21. Oct 2015).

NGCert (2015). *Next Generation Certification.* URL: www.ngcert.eu (visited on 13. Nov 2015).

Pearson, S. (2011). Toward Accountability in the Cloud. *IEEE Internet Computing*, 15 (4), 64–69.

Pedrosa, I. and C. J. Costa (2014). "New trends on CAATTs." In: *Proceedings of the International Conference on Information Systems and Design of Communication*, 138–142.

Pichan, A., Lazarescu, M. and S. Teng Soh (2015). Cloud forensics. *Digital Investigation*, 1338–57.

Porter, M.E. (2004). *Competitive advantage.* 1st Free Press Export Edition. Free Press, New York, London.

Postel, J. (1981). RFC: 791 - Internet Protocol: DARPA Inernet Programm, Protocol Specification.

Praeg, C.-P. and U. Schnabel (2006). "IT-Service Cachet - Managing IT-Service Performance and IT-Service Quality." In: *Proceedings of the 39th Annual Hawaii International Conference on System Sciences - Volume 02*. IEEE Computer Society, Washington, DC, USA, 1–34.

Rajalakshmi, J.R., Rathinraj, M. and M. Braveen (2014). "Anonymizing log management process for secure logging in the cloud." In: *Circuit, Poartwer and Computing Technologies*, 1559–1564.

Rezaee, Z., Sharbatoghlie, A., Elam, R. and P. L. McMickle (2002). Continuous auditing. *Auditing*, 21 (1), 147–163.

Rogers, E.M. (1962). *Diffusion of innovations.* 1st Edition. Free Press, New York.

Rogers, E.M. and F. F. Shoemaker (1971). *Communication of Innovations: A Cross-Cultural Approach.* 2nd Edition. Free Press, New York.

Rogers, E.M. (1983). *Diffusion of innovations.* 3rd Edition. Free Press, New York.

Rogers, E.M. (2003). *Diffusion of innovations.* 5th Edition. Free Press, New York.

Schneider, S. and A. Sunyaev (2016). Determinant factors of cloud-sourcing decisions: reflecting on the IT outsourcing literature in the era of cloud computing. *Journal of Information Technology*, 31 (1), 1–31.

Schwartz (2011). *Epsilon Fell To Spear-Phishing Attack: Breach apparently lasted for months despite warning of targeted attacks against email service providers.* URL: www.darkreading.com/attacks-and-breaches/epsilon-fell-to-spear-phishing-attack/d/d-id/1097119 (visited on 25.11.2015).

Shin, I., Lee, M. and W. Park (2013). Implementation of the continuous auditing system in the ERP-based environment. *Managerial Auditing Journal*, 28 (7), 592–627.

Singh, K., Best, P.J., Bojilov, M. and C. Blunt (2013). Continuous auditing and continuous monitoring in ERP environments. *Journal of Information Systems*, 28 (1), 287–310.

Stephanow, P. and N. Fallenbeck (2015). "Towards continuous certification of Infrastructure-as-a-service using low-level metrics." In: *International Conference on Advanced and Trusted Computing*, 1–8.

Stephanow, P., Banse, C. and J. Schütte (2016). "Generating Threat Profiles for Cloud Service Certification Systems." In: *17th IEEE High Assurance Systems Engineering Symposium (HASE)*.

Sturm, B., Lansing, J. and A. Sunyaev (2014). "Moving in the Right Direction?: Mapping Literature on Cloud Service Certifications' Outcomes with Practitioners' Perceptions." In: *Proceedings of the 22nd European Conference on Information Systems*, Tel Aviv, Israel.

Subashini, S. and V. Kavitha (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Netwwork and Computer Applications*, 34 (1), 1–11.

Sun, T., Alles, M. and M. A. Vasarhelyi (2015). Adopting continuous auditing: A cross-sectional comparison between China and the United States. *Managerial Auditing Journal*, 30 (2), 176–204.

Sunyaev, A. and S. Schneider (2013). Cloud services certification. *Communications of the ACM*, 56 (2), 33–36.

Swanson, E.B. and N. C. Ramiller (1997). The Organizing Vision in Information Systems Innovation. *Organization Science*, 8 (5), 458–474.

Tornatzky, L.G. and K. J. Klein (1982). Innovation characteristics and innovation adoption-implementation: A meta-analysis of findings. *IEEE Transactions on Engineering Management*, EM-29 (1), 28–45.

Vasarhelyi, M.A. and F. B. Halper (1991). The continuous audit of online systems. *Auditing*, 10 (1), 110–125.

Vasarhelyi, M.A., Alles, M.G., Kogan, A. and D. O'Leary (2004). Principles of analytic monitoring for continuous assurance. *Journal of Emerging Technologies in Accounting*, 1 (1), 1–21.

Vasarhelyi, M.A., Alles, M., Kuenkaikaew, S. and J. Littley (2012). The acceptance and adoption of continuous auditing by internal auditors. *Methodologies in AIS Research*, 13 (3), 267–281.

Wang, B., Li, B. and H. Li (2014). Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud. *IEEE Transactions on Cloud Computing*, 2 (1), 43–56.

Webster, J. and R. T. Watson (2002). Analyzing the Past to Prepare for the Future. *Management Information Systems Quarterly*, 26 (2), xiii.

Wolf, M.-B. and J. Rahn (2015). "Empirical Qualitative Analysis of the Current Cloud Computing Market for Logistics." In: *Cloud Computing for Logistics . Ed. by* M. ten Hompel; J. Rehof; O. Wolf. Springer International Publishing, 29–44.

Woodroof, J. and D. Searcy (2001). "Continuous audit implications of internet technology." In: *Hawaii International Conference on System Sciences*, 1–8.

Wu, J.-H. and S.-C. Wang (2005). What drives mobile commerce?: An empirical evaluation of the revised technology acceptance model. *Information & Management*, 42 (5), 719–729.

Yeh, C.-H., Chang, T.-P. and W.-C. Shen (2008). "Developing continuous audit and integrating information technology in e-business." In: *Asia-Pacific Services Computing Conference*, 1013–1018.

Zaltman, G., Duncan, R. and J. Holbek (1973). *Innovations and organizations.* Wiley, New York.

Zhang, H. (2005). Trust Promoting Seals in Electronic Markets: Impact on Online Shopping Decisions, 6 (4).