Trust is Good, Control is Better: Creating Secure Clouds by Continuous Auditing

Sebastian Lins, Stephan Schneider, and Ali Sunyaev

Abstract—Cloud service certifications (CSC) attempt to assure a high level of security and compliance. However, considering that cloud services are part of an ever-changing environment, multi-year validity periods may put in doubt reliability of such certifications. We argue that continuous auditing (CA) of selected certification criteria is required to assure continuously reliable and secure cloud services, and thereby increase trustworthiness of certifications. CA of cloud services is still in its infancy, thus, we conducted a thorough literature review, interviews, and workshops with practitioners to conceptualize an architecture for continuous cloud service auditing. Our study shows that various criteria should be continuously audited. Yet, we reveal that most of existing methodologies are not applicable for third party auditing purposes. Therefore, we propose a conceptual CA architecture, and highlight important components and processes that have to be implemented. Finally, we discuss benefits and challenges that have to be tackled to diffuse the concept of continuous cloud service auditing. We contribute to knowledge and practice by providing applicable internal and third party auditing methodologies for auditors and providers, linked together in a conceptual architecture. Further on, we provide groundings for future research to implement CA in cloud service contexts.

Index Terms—Certification, cloud computing, continuous auditing, security

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. However, organizations are still hesitant to adopt cloud services because of security, privacy, and reliability concerns regarding provisioned cloud services as well as doubts about trustworthiness of their cloud service provider [1], [2], [3]. Cloud service certifications (CSC) are good means to address these concerns by establishing trust, and increasing transparency of the cloud market [2], [4]. Several CSC have evolved, such as *CSA STAR* or *EuroCloud Star Audit*. These CSC attempt to assure a high level of security, reliability, and legal compliance, for a validity period of one to three years. However, cloud services are part of an ever-changing environment, resulting from fast technology life cycles and inherent cloud computing (CC) characteristics, like on-demand provisioning and entangled supply chains [5], [6]. Hence, such long validity periods may put in doubt reliability of issued certifications. CSC criteria may no longer be met throughout these periods, for instance, due to configuration changes or major security incidents. Thus, continuous auditing (CA) of certification criteria is required to assure transparent, continuously reliable, and secure cloud services and to establish a trustworthy CSC after the initial certification process is accomplished.

Extant research has focused on implementing and evaluating CA of information systems since the early nineties. This progression has included the evolution of architecturally different methodologies, for instance, embedded audit modules [7] and independent monitoring control layers [8], which help to monitor and audit information systems. However, past research has mostly examined CA for internal purposes only. In the context of CC, researchers recently proposed the means to enable third party authorities to audit data integrity [9], data location compliance [10], and changes of cloud infrastructure [11] among others. Aside from these special purpose methodologies, research currently lacks a comprehensive architecture, enabling third party auditors to continuously audit a broad variety of CSC criteria.

We address this gap by conceptualizing an architecture for CA of cloud services, comprising main components, methods, and processes while considering the requirements and needs of main stakeholders. Before conceptualizing an architecture, and thus defining how to perform CA, it has to be analyzed where CA is reasonable. Subsequently, we analyze which CSC criteria should be continuously audited to assure ongoing adherence by performing workshops with cloud service auditors first. Then, we evaluate how these criteria can be continuously audited to identify main auditing components and methodologies for our proposed architecture. Therefore, we build on and extend previous work on CA methodologies by Lins et al. [12]. To ensure applicability of considered methodologies in the CC context, we conducted three expert interviews with cloud service auditors. To link methodologies and to discuss potential architectures as well as to consider stakeholder requirements, we conducted three workshops with cloud service providers, consultants, and auditors as well as ten semi-structured interviews with cloud service customers. Finally, based

- *The authors are with the Department of Information Systems, University of Cologne, Cologne, Germany.*
  E-mail: {lins, schneider, sunyaev}@wiso.uni-koeln.de.

Manuscript received 16 Oct. 2015; revised 4 Jan. 2016; accepted 24 Jan. 2016. Date of publication 27 Jan. 2016; date of current version 31 Aug. 2018.
Recommended for acceptance by J.H. Abawajy.
For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TCC.2016.2522411

upon these findings, we conceptualize an architecture to continuously audit cloud services in a practically and economically feasible manner. Summing up, we focus on the following objectives within this study:

i. Which CSC criteria should be continuously audited?
ii. Which CA methodologies exist and are applicable in the context of continuous cloud service auditing?
iii. How can methodologies be linked together to form an architecture which enables CA?

Our findings reveal that various CSC criteria (e.g., performing regular vulnerability testing and ensuring data integrity) should be continuously audited to assure ongoing certification adherence and to prove secure and reliable services. Moreover, interviews revealed that most of existing methodologies are not applicable for (external) third party auditing purposes. Therefore, providers have to establish an internal auditing department, which manages provision of audit-relevant data. Finally, our conceptual architecture highlights important components (i.e., various interfaces and auditing management modules) as well as processes that have to be implemented. We thereby contribute to practice and research in several ways:

1. We support cloud auditors to classify whether or not a high frequency auditing of their CSC criteria is required. Further on, we illustrate methodologies which can be used by auditors to perform (external) auditing of cloud services as well as by cloud service providers to set up an internal auditing department.
2. We transfer the concept of CA in a new context, provide means and foundations for further research, and demonstrated benefits, challenges, and limitations of CA of cloud services.
3. By providing a first conceptual architecture, we want to encourage auditors and cloud service providers to implement CA techniques, consequently creating trustworthy certifications and services.

This paper proceeds as follows. We first provide a background on CC, CA, and related work, followed by a presentation of our research approach. In Section 4, we briefly evaluate what criteria should be continuously audited. In Section 5, we discuss identified methodologies. In Section 6, we present our architecture for CA of cloud services. We then discuss challenges and benefits in Section 7 and 8 as well as conclude with directions for future research.

2 Background

2.1 Cloud Computing and Certification

Cloud computing enables ubiquitous, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [13]. These resources refer, for instance, to hardware, development platforms, and applications. CC entails five essential characteristics, that are: 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. These characteristics challenge current assessment processes [6]. Therefrom, CC faces a broad range of security issues, including accessibility vulnerabilities, privacy, and control issues as well as issues related to data integrity and data confidentiality [1].

Extant research already proposes certifications and audits as detective controls and good means to assess quality and performance of IT services in procurement processes [2], [4], [14]. A certification is defined as a third party attestation of products, processes, systems, or persons that verifies conformity to specified criteria [15]. Several CSC (e.g., *CSA STAR*) and cloud certification schemes in particular (e.g., *ISO 27017*) have emerged to assure a high level of security, reliability, and legal compliance of cloud services. Recent research suggests that CA is required to deal with the ever-changing environment of cloud services and to increase trustworthiness of CSC [6], [16], [17].

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 [18]. Thus, CA enables auditors to immediately react to changes or events concerning the subject matter and to adjust their auditing reports based on assessment of these changes and events.

The early works of Groomer and Murthy (1989) concerning implementation of embedded audit modules [7] and Vasarhelyi and Halper (1991) regarding usage of monitoring and control layers [8] spawned a research stream of CA. Therefrom, extant literature investigates implementation, transferability, and diffusion of CA in varying domains [19], [20], [21]. Recently, researchers discussed CA of enterprise resource planning systems [22], [23], accounting systems [24], [25], and web services [26], [27]. In the context of CC, research started to propose different approaches to enable third party auditing, for example, methodologies to enable auditors to simultaneously verify integrity of multiple users' data [9] and to assure data location compliance by analyzing audit logs [10]. However, a comprehensive CA architecture, which is able to audit a broad range of CSC criteria and combines various methodologies, is still missing.

2.3 Related Work

Extant research has already focused on automation of assessment and certification approaches in the context of service oriented architectures. For example, Lamparter et al. demonstrate how to automatically evaluate whether a web service execution meets contract requirements [28]. Ardagna et al. propose a machine-readable certification, which is issued to the service after validating its reliability properties [29]. Stephanow and Fallenbeck demonstrate how metrics can serve to support continuous validation of generic CSC criteria [17], [30], [31]. Lins et al. reviewed various automated auditing and monitoring methodologies, and briefly evaluate their applicability in the context of cloud computing [12]. Further on, a variety of research focuses on developing and analyzing cloud architectures (e.g., [32], [33]) to enable continuous monitoring of cloud services. Continuous monitoring is defined as ongoing observance and analysis of operational states of systems and applications to provide decision support, detect and diagnose problems, and to

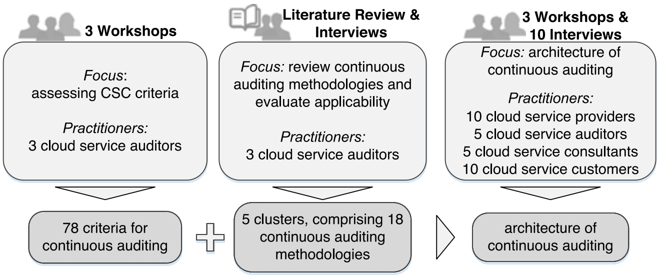
3 Workshops
Focus: assessing CSC criteria
Practitioners: 3 cloud service auditors
Literature Review & Interviews
Focus: review continuous auditing methodologies and evaluate applicability
Practitioners: 3 cloud service auditors
3 Workshops & 10 Interviews
Focus: architecture of continuous auditing
Practitioners: 10 cloud service providers 5 cloud service auditors 5 cloud service consultants 10 cloud service customers
78 criteria for continuous auditing
5 clusters, comprising 18 continuous auditing methodologies
architecture of continuous auditing

Fig. 1. Overview of research approach.

provide information for further analyses [33] and is performed by service providers or a third party. Consequently, continuous monitoring approaches are designed for internal monitoring purposes only, and gathered monitoring information is kept in-house to be solely inspected by system administrators. Hence, in contrast to CA, monitoring of CC infrastructures does not provide any proof to customers that provided services are reliable and secure.

3 Research Approach

To gain practical insights into CSC auditing processes and to get access to expertise and experience of practitioners, we cooperated with *CloudAuditor*, an auditing company offering global, independent quality and safety inspection services as well as a CSC, which is becoming increasingly relevant across Europe.

To answer the research questions, we apply a three-step research approach (see Fig. 1). We first conducted workshops with practitioners from *CloudAuditor* to assess CSC criteria. Second, we build on and extend previous research on CA methodologies [12] and conducted interviews with *CloudAuditor* practitioners to evaluate their applicability in the context of CC. Finally, we held three workshops with cloud service industry experts as well as ten interviews with cloud customers to elicit requirements and conceptualize an architecture of CA of cloud services.

3.1 Assessing Certification Criteria

Before conceptualizing an architecture for CA, we specify which cloud service parameters, components, and processes have to be continuously audited to assure ongoing secure cloud services. Therefore, we assessed which criteria require a high frequency auditing after the initial certification process was accomplished.

To take a variety of CSC criteria into consideration, we included two different CSC criteria catalogues: the criteria catalogue from *CloudAuditor* (comprising 273 criteria) and the CSC criteria taxonomy from Schneider et al. (comprising 328 criteria) [16]. For further analysis, the authors and practitioners from *CloudAuditor* jointly merged both catalogues to reduce redundancies and irrelevant criteria. As a result, the final criteria collection comprised 326 CSC criteria.

Three workshops were held with *CloudAuditor* practitioners to jointly assess each criterion whether or not a high frequency auditing is required. The workshops lasted about two hours on average. In total, 78 out of 326 certification criteria were marked as a candidate for CA. Finally, for each criterion an auditing frequency was proposed based upon their experience from conducting cloud service audits and their technical knowledge. Results of the joint assessments are presented in Section 4.

3.2 Assessing Continuous Auditing Methodologies

In previous work, Lins et al. performed a comprehensive literature review to identify (semi-) automated auditing methods that are applicable in the context of cloud computing [12]. Their study yields a set of (semi-) automated methods for continuous monitoring and auditing in six clusters. We build on their findings and further extend their literature review by extending their search string and performing a backward and forward analysis. Therefrom, 18 CA methodologies from 66 research articles were extracted, which will be discussed in Section 5. A detailed explanation on why and how we extend their findings can be found in Appendix A, which can be found on the Computer Society Digital Library at http://doi.ieeecomputersociety.org/10.1109/ TCC.2016.2522411.

After identifying methodologies, their practical applicability in context of cloud service auditing needed to be assessed. Therefore, semi-structured one-on-one interviews with practitioners from *CloudAuditor* were conducted. Interviews allow gathering of rich data from people in different roles [34]. Furthermore semi-structured interviews involve use of pre-formulated questions, but allow improvisation for emerging topics during conversation as well. In total, three semi-structured interviews were conducted with two security analysts and one certification consultant, lasting about 80 minutes in average and 4 hours in total. Interview guidelines were prepared individually beforehand and started with general questions concerning execution of auditing processes followed by descriptions of selected methods and questions regarding their feasibility and applicability (see Appendix E, available in the online supplementary material). All interviews were approved to be recorded and transcribed afterwards. Applicability assessments were analyzed and are presented in Section 5.

3.3 Conceptualizing an Architecture for Continuous Auditing

To link identified methodologies, to discuss potential architectural concepts and to consider stakeholder requirements, we conducted three workshops with cloud service experts following the qualitative research method of focus group interviews. 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 certain experiences [34]. Furthermore, focus groups allow participants to engage in thoughtful discussions, hence generating practical oriented and rich data. During these workshops, the concept of CA was lively discussed and exemplarily transferred to individual use cases of practitioners. In total, ten cloud service providers, nine cloud service auditors, and five cloud service consultants participated. The different cloud service providers operate on a national and global scale, providing infrastructure, platform, and software as a service. 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 authorities, 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. A workshop lasted on average 4 hours and 30 minutes and all three workshops lasted 15 hours in total. Since no cloud service customer participated during these workshops, consultants and providers were asked to represent a customer's perspective and to report on their experience with customers. In addition, we conducted 10 semi-structured one-on-one interviews with cloud service customers. Interviewees are IT managers from medium to large enterprises and different sectors including IT, health, trade, and finance, which use various cloud service models. An interview lasted on average 60 minutes. Appendix E, available in the online supplementary material, illustrates interview guidelines for (focus group) interviews with auditors, providers, and customers.

Interviews were recorded, transcribed, and analyzed by three researchers independently, applying qualitative data coding techniques [34] (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 new components, processes, and relationships based on data collected. With the goal to conceptualize an architecture, we were particularly interested in understanding potential components and processes as well as relationships and requirements which have to be considered when conceptualizing an architecture. On the second stage of analysis (axial coding), we used components, methods, and architectures assessed in the Section 5 while analyzing transcripts to confirm that these accurately represent interview responses and to explore how they are related to findings from the open coding stage. Finally, based on insights gained during this coding analyses and practitioner discussions during workshops and interviews, a conceptual architecture of CA were derived comprising of necessary processes and components to assure ongoing certification adherence.

4 Continuous Auditing Criteria

Existing CSC represent only a retrospective look at the fulfillment of technical and organizational measures at the time of their issuing. CSC criteria may no longer be met throughout certification validity periods. Current CSC are facing several drawbacks when assuring ongoing certification adherence, including:

a. *Inherent cloud computing characteristics.* Cloud services are part of an ever-changing environment, resulting from inherent CC characteristics, like on-demand provisioning and entangled supply chains. Furthermore, cloud services are characterized by fast technology life cycles compared to other industries.

b. *Ongoing architectural changes.* Hardware or software configuration changes as well as changing sub service providers might lead to certification violations or security vulnerabilities. Such security vulnerabilities could go undetected for a long time without appropriate monitoring mechanisms. Especially in case of performing agile software development and providing cloud applications, current certifications are lacking capabilities to observe and deal with continuous deployments.

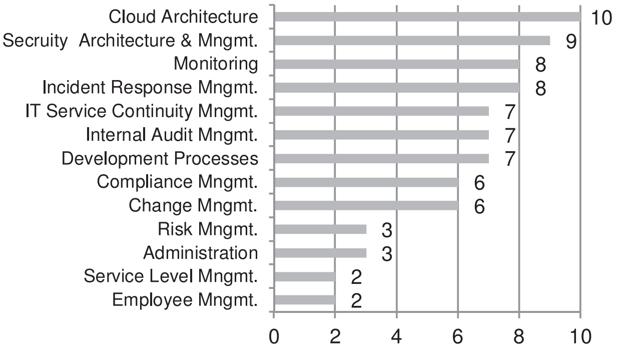

Fig. 2. Categories of criteria that were marked for CA.

c. *Environmental threats.* Changes in the CC and IT environment, for example emergence of new vulnerabilities, require providers to adapt their services to cope with emerging challenges. Major security incidents may threaten the service or reveal harmful vulnerabilities, which in turn void a certification.

d. *Changes in legal and regulatory landscape.* The legal and regulatory landscape of cloud services is highly dynamic since existing laws are currently adjusted, and new laws are being proposed to cope with challenges resulting from the digital transformation of society and continuous changes in IT. Just recently, the Safe Harbor data sharing agreement between the European Union and the United States was questioned. These dynamics might change responsibilities of both cloud service customers and providers as well as require certification criteria to be successively updated.

e. *Deliberate discontinuance.* A cloud service provider might deliberately discontinue adherence to CSC criteria to achieve benefits (e.g., cost savings).

Assessments during the workshop revealed that 78 of 326 certification criteria should be continuously audited since they are affected by at least one of these drawbacks. For example, a CSC criterion states that '*source code reviews should be performed regularly to identify possible vulnerabilities and security issues when developing software*'. Since this criterion implies actions, which have to be performed on a regular basis, cloud service providers might deliberate discontinue fulfilling this criterion to save costs. Appendix B, available in the online supplementary material, provides a checklist to assess CSC criteria and corresponding examples. Additionally, Appendix C, available in the online supplementary material, summarizes findings regarding potential frequencies of CA.

Criteria were further grouped into different categories based upon their requirement contexts. Fig. 2 lists these categories and the number of criteria contained. Interviews with customers confirm that especially criteria ensuring service availability, data integrity and location, a secure access management, and data encryption should be continuously audited. These criteria are reflected by the following categories, which will be briefly outlined.

First, criteria of category *Cloud Architecture* ensures ongoing network security, performing backups and assure secure multi-tenancy capabilities. Second, criteria in category *Security Architecture and Management* necessitate performing

TABLE 1
Clusters of Identified CA Methodologies

Computer-Assisted Auditing Tools and Technologies (CAATT)
Packaged and automated auditing processes that enable auditors to extract, sample, and analyze auditees' data.

Evidence Gathering Mechanisms
Mechanisms to gather and store electronic evidence and information, for example, embedded audit modules or digital agents.

Auditing System Architectures
Architectural concepts to design and to perform CA.

Log Inspection
Inspect logs, which contain information about system operation.

Data Integrity Validation
Methods to audit integrity of customer data stored in a cloud.

continuously vulnerability analysis and assuring encrypted data storage, data confidentiality and integrity. Moreover, *Monitoring* compromises criteria, which require ongoing monitoring of service availability, cloud components, and networks. *Incident Response Management* contains criteria that require providers to receive and process incident messages in a timely manner. Further criteria belonging to category *IT Service Continuity Management* require providers to test, extend, and update service and business continuity plans regularly. Criteria assigned to category *Internal Audit Management* necessitate providers to audit potential subproviders, perform and evaluate technical audits. Concerning *Development Processes*, documenting code, performing code reviews, and assuring secure development processes should be continuously audited. Ongoing *Compliance Management* assures compliant data location and service adjustments due to changes of legal or regulatory requirements. *Change management* implies performing (security) tests before integrating new hardware components and software as well as performing patch management processes. Furthermore, *Risk Management* requires providers to perform ongoing risks analyses, reviews, and updates of risk management plans. Criteria contained in category *Administration* ensure performing regular administration tasks, for example, deletion of inactive user accounts. *Service Level Management* implies monitoring and reporting of service level agreements adherence. Finally, *Employee Management* contains criteria that recommend performing regular employee trainings.

This brief outline approves that various CSC criteria should be continuously audited to assure permanent secure cloud services since they can be affected by different influences (e.g., environmental threats). These criteria address different areas, demand individual audit-evidence, and hence require various CA methods.

5 Continuous Auditing Methodologies

In this section, identified CA methodologies are presented and discussed according to their applicability in CC contexts. Methodologies were clustered regarding their objectives and application contexts (see Table 1). Appendix D, available in the online supplementary material, provides an overview of identified methodologies.

5.1 Computer-Assisted Auditing Tools and Technologies

Since the 1980s, researchers and practitioners have developed various computer-assisted auditing tools and technologies which might support CA [35], [36]. Computer-assisted auditing tools can be used by an auditor as part of their audit procedures to connect to an auditee's information system, automatically extract, sample, and analyze necessary data [37]. These tools comprise generalized auditing software, electronic working papers, and tools for fraud detection among others [38], [39]. More importantly, CA functions were recently added to these tools. However, existing computer-assisted auditing tools are mainly used in and developed for accounting contexts [35], [36], [39]. Hence, their applicability in CC contexts might be questionable. Likewise, interviews revealed that in CSC auditing practice computer-assisted auditing tools are mainly used to support technical security analyses, for instance, penetration tests and vulnerability scans.

Regularly performing penetration tests and vulnerability scans are recommended by auditors and demanded by customers to validate adequate security mechanisms and to identify system vulnerabilities. By attempting to execute prohibited behavior or attacks on vulnerabilities, auditors can verify that such behavior is prevented or detected and compensated. A broad variety of corporate and open-source tools exist to support efficient penetration testing and vulnerability scanning (e.g., *Qualys*). These tools provide a variety of (semi-) automated functions (e.g., scan network ports, identify running services, analyze and test well-known vulnerabilities), and can be individually configured based upon an auditee's context. Performing extensive penetration tests on a continuous basis (e.g., weekly) might be limited since they still require high manual efforts. Thus, future research should evaluate how to design automated auditing processes that use penetration tests to validate security measures.

Aside from emergence of a broad variety of tools, important technological advances enhanced technological feasibility of CA [40]. The introduction of XML, the development of the '*Extensible Business Reporting Language*', and its extension '*Global Ledger*' enabled a platform independent, efficient, and effective exchange of business information over the Internet [27], [40]. Practitioners recommend using XML-coded data when exchanging data between auditee and auditor, because XML-coded data is standardized, well-structured, and can be processed quickly. Similar, a broad variety of formal languages can be used to facilitate CA. For example, the '*Open Vulnerability and Assessment Language*' can be used to enable semi-automated patch and configuration management validation, and vulnerability assessments [41].

5.2 Evidence Gathering Mechanisms

Several automated methodologies have been identified to enable auditors to gather electronic audit evidence. The most frequently mentioned component to gather audit evidence is an embedded audit module (EAM). EAM are special purpose functions, programs, or other code objects that are embedded into auditees' information systems and supervise all of audit-related data in real-time [7], [35], [42], [43], [44], [45], [46], [47]. One of the most important advantages of

EAM is that they automatically act as triggers and inform the auditor when suspicious events appear, thus eliminating the need for high frequency assurance queries [7], [35], [42]. Recently, organizations have begun to equip EAM with artificial intelligence to expand their capabilities [46]. However, EAM are more vulnerable to manipulation, especially by auditees' employees who have necessary access privileges to interfere [7], [42]. In the context of CC, an EAM might be used, for example, to monitor reliability and availability [29]. Nonetheless, usage of EAM for continuous cloud auditing may be limited because incorporation of EAM into a cloud architecture (that is distributed across different datacenters and locations) requires a complicated, expensive development and customization process [7], [12], [24], [42]. More importantly, practitioners assess that usage of EAM might not be feasible. First of all, most auditees are not willing to permit auditors to integrate third party IT components due to security and privacy concerns since they might cause new security vulnerabilities or disturb system operation. Auditees might even fear data theft or corporate espionage. Moreover, integrating EAM might violate internal compliance requirements or corporate security policies. Practitioners empathized that usage of EAM seems to be exclusively feasible, if these EAM require minimal access privileges and analyze non-confidential data. Hence, practitioners and researchers need to evaluate how EAM might be implemented while ensuring confidential data gathering and exchange with auditors.

Alternatively, digital agents can support auditing processes [11], [21], [35], [48], [49], [50]. Digital agents (also referred to software, autonomous, or intelligent agents) are software objects that achieve individual goals by autonomously performing actions and reacting to events in a dynamic environment. They are characterized by having different degrees of artificial intelligence and mobility (the ability to travel from one platform to another) [35], [49]. In contrast to EAM, digital agents remain on the auditor's side and are only deployed to the auditee's infrastructure during auditing processes. Digital agents are supposed to automatically perform activities that are traditionally undertaken by human auditors, for example, collecting audit evidence, and validating certification criteria [21], [35], [49]. Typically, audit tasks are performed by a team of agents, which are hierarchically structured [11], [51]. Through their artificial intelligence, mobility, and individual, autonomous acting, they seem to be very suitable for continuous cloud service auditing, especially when comparing digital agents to EAM. However, high efforts and expenses for agent development and implementation as well as possible negative impacts on system performance have to be considered [35]. Similar to EAM, usage of digital agents has been evaluated critically by practitioners: "*I think that customer acceptance to permit digital agents is very low because with these agents you implement untrustworthy software into your cloud systems*" [Auditor]. Especially agent deployment interfaces might be a highly valuable target for attackers to compromise auditees' and auditors' systems. Thus, future research should evaluate how to address potential security vulnerabilities when using (third party) digital agents (e.g., sharing encryption keys between agents and data sources to enable authentication [52]).

Furthermore, an interceptor can be applied as a wrapper that is used to encapsulate information systems or IT components [24], [53]. They can monitor data flowing into and out of systems, therefore enabling CA. Interceptors can be configured to validate accordance with implemented business logics and certification criteria [54]. Contrary to EAM, interceptors usually operate independently of information systems. Hence, they can be implemented in any phase of a software life cycle, and detailed knowledge about auditees' information systems are not necessary to initiate an interceptor. Currently, different vendors offer a variety of tools to implement interceptors on different system layers to capture messages (e.g., *Apache Axis handler* for the middleware layer) [24]. Practitioners are currently using interceptor tools (e.g., *Burp Suite*) to intercept data streams between cloud servers and their web browsers to identify and test security vulnerabilities. Auditors suggest that interceptors can be used for CA of cloud services. However, when implementing interceptors for CA, one has to filter and adjust the amount of data that is actually analyzed to prevent performance losses, security and privacy concerns (e.g., fear of monitoring employees).

Further on, CA systems may incorporate different data, text, and process mining techniques, which are performed on a regularly basis to extract audit evidence [46], [55], [56]. Data mining techniques try to discover patterns in large sets of data and to detect irregularities. Text mining involves discerning patterns from text to detect deception and fraud, and can be applied, for example, to email, discussion groups, media, and in general to the Internet. These mining techniques can be used, for example, to detect changes in auditees' system architecture. Moreover, auditors need to identify and evaluate external changes, for example, emergence of security threats or vulnerabilities, which might trigger re-auditing events or alerts. Mining techniques can be used to assess open vulnerability databases (e.g., *Common Vulnerability and Exposures Database*) to expose unknown vulnerabilities and system weakness configurations that may cause system crashes and malfunctions [55]. Finally, by using process mining techniques auditors can gain insights into how processes are being undertaken by analyzing a vast amount of data that is routinely gathered and stored in event logs [56]. Process mining compares actually logged process with a designed process model. Interviews revealed that such process mining techniques might bear great potential to continuously audit and confirm process executions. Yet, comparison of derived and designed process models might be limited since most auditees do not provide models in suitable, machine-readable formats to enable an automated model comparison. Hence, future research should evaluate how process mining techniques might be used in the CA contexts, for example, by using training log files to automatically and continuously create process models [57].

5.3 Auditing System Architectures

To enable a continuous evidence extraction and transmission, a communication model is required. An auditor's system can be efficiently connected to auditees' systems, for example, by using the *Simple Object Access Protocol* to exchange messages, or by using the *Common Object Request*

Broker Architecture as a middleware to gather information from heterogeneous auditees' applications [58]. Audit-relevant data can be transferred at predetermined intervals and then stored in supplementary databases, for instance, in audit data marts [22], [45], [51]. Audit data marts are small, mostly auditee-independent data repositories in which relevant data is automatically stored, enabling real-time data access and automated data analyses [45].

Aside from individual mechanisms to gather audit evidence, researchers have developed several comprehensive CA system architectures. A monitoring and control layer can be implemented as an independent auditing system [23], [42]. This system forms an overlay on top of a set of existing systems and utilizes a middleware layer to provide integration between loosely coupled applications such as auditees' service applications and legacy systems [23], [25], [59]. Data from integrated applications can be extracted and compared to a predefined auditing rule-set, and detected violations might automatically trigger an alert. This system is owned and operated by the auditor, thus data retrieved can be presumed to be tamper-proof [23], [42]. Applicability of monitoring and control layers in CC contexts might be limited due to distributed cloud infrastructures.

Besides, agent-based CA architectures are common in literature and practice. Under this architecture, a digital agent is initiated to represent a certain audit procedure and dispatched to different auditees' systems [35], [51]. A flexible (e.g., platform independent) and adaptable (e.g., agent can be deployed as required) agent-based architecture facilitates gathering audit evidence in distributed and heterogeneous auditees' systems [60]. Hierarchically structured teams of agents will perform planned audit operations, for example, interacting with an auditee's system and retrieving necessary audit evidence, testing effectiveness of business processes, or mining data to analyze and identify fraud behavior [11], [51]. In contrast to usage of monitoring and control layers in cloud contexts, agent-based CA architectures enable a flexible deployment and transmission of agents across different cloud infrastructures and locations.

Furthermore, CA can be implemented as a set of web services that reside within an auditor's computing environment [26], [27], [40]. Each auditing function is therefore represented as a web service which can be invoked to continuously audit an auditee's system [27]. Usage of web services for auditing enables new business models for auditors, for example, cloud customers paying a service fee for invoking an auditor's web service to continuously retrieve assurance reports. In this regard, an incident detection web service was developed to enable customers to observe individual specified security and monitoring policies [11].

When performing CA, a huge volume of data, exceptions and reports may be generated, thus threatening audit efficiency. To counteract this issue, it is recommended to implement decision support systems (DSS) [46]. Such systems might enhance CA by aggregating information from many different sources (e.g., agents or minded data), reacting on auditee reports, and by efficiently and automatically deciding to take actions or to alert the auditor. Consequently, DSS ultimately reduce workload of auditors. Future DSS may even evolve to intelligent and adaptive audit process systems, which automatically adjust audit tests based on gathered data and unexpected events [46]. Interviews revealed that DSS are currently not used during CSC processes. Nonetheless, auditors endorse the concept of using these systems to support and to automate their auditing.

5.4 Log Inspection

Interviews revealed that auditors agree to inspect logs, which are routinely created during monitoring operations by services providers to assess certification adherence. In the following, exemplary log inspection techniques will be presented. To monitor execution of applications, abstract execution logs can be inspected by using heuristics-based log inspection techniques [61]. Such techniques can inspect log lines with limited format requirements and can scale up to process log files, which contain millions of log lines. Supposedly, such a method can be used to automatically and continuously check whether different applications are actually running on a cloud infrastructure, for example, malware protection or antivirus software [12]. Likewise, unstructured logs can be automatically analyzed, for example, to detect system anomalies [57]. To analyze unstructured logs, data mining techniques can be used, comprising learning and detection process. During learning processes, ideal models that represent the normal executional behavior of the system are derived based upon training log files. In detection processes, new input logs are compared to the ideal models to automatically detect anomalies. Further on, logs can be analyzed to assure protection of customers' privacy a posteriori [62]. To implement such techniques, a policy language for expression of privacy preferences (e.g., access regulations) and an automated process for checking adherence to policies (e.g., tree pruning strategies [63]) have to be implemented [62].

5.5 Data Integrity Validation

As cloud service customers do not longer possess their data locally, assuring that their data is being correctly stored and integrity is maintained in cloud environments is of critical importance. Data integrity may be threatened by, for example, malicious insiders, data loss, technical failures, and by external attackers [64]. To create trustworthy cloud services, auditors should continuously validate that data integrity is maintained.

A wide range of research currently addresses the question on how to assure data integrity by a third party in CC contexts. Especially hashing techniques have been identified as adequate methods for monitoring integrity of large amounts of data [65], [66], [67]. These techniques enable auditors to simultaneously verify integrity of multiple users' data, which is important in multitenant cloud environments with many users operating at the same time. Moreover, simultaneous monitoring of multiple and hybrid clouds, and multiple owners is feasible [65]. Aside from that, some methods support dynamic data operations on a fine-grained level, thus, minor data changes are considered when validating data integrity [67]. Data security and privacy has to be ensured when validating data integrity in cloud environments, for example, by implementing cryptography [65], authentication [64], or authorization techniques [66], [67]. Furthermore, auditors can reduce communication and computation cost by using periodic sampling audits [66], or moving computational operations onto cloud servers [65]. Scenarios in which cloud users

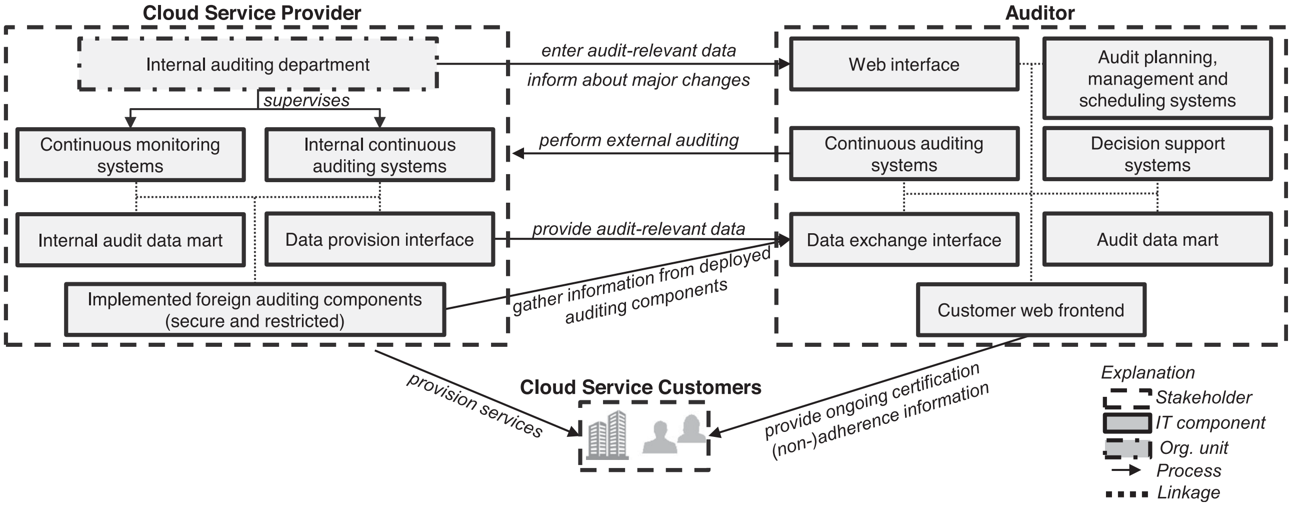
Cloud Service Provider
Internal auditing department
supervises
Continuous monitoring systems
Internal continuous auditing systems
Internal audit data mart
Data provision interface
Implemented foreign auditing components (secure and restricted)
enter audit-relevant data
inform about major changes
perform external auditing
provide audit-relevant data
gather information from deployed auditing components
Auditor
Web interface
Audit planning, management and scheduling systems
Continuous auditing systems
Decision support systems
Data exchange interface
Audit data mart
Customer web frontend
provision services
Cloud Service Customers
provide ongoing certification (non-)adherence information
Explanation
Stakeholder
IT component
Org. unit
Process
Linkage

Fig. 3. Conceptual architecture for continuous auditing.

are sharing data as a group require adjusted integrity validation checks since auditors may be able to reveal confidential information of the group by traditional approaches (e.g., which user in the group is modifying data most) [9], [68]. Auditors can use private group keys as additional file signatures and index tables to ensure data integrity in shared data contexts [9], [68].

When stored data is archived, it remains necessary to ensure its integrity for disaster recovery or to assure compliance with legal requirements [69]. To perform automatic integrity checks, a data integrity protection scheme is proposed [69]. Given an archive file, it can be encoded into code chunks, which are distributed over and stored on a number of servers. An auditor can ask for randomly chosen parts of remotely stored data, and run a probability checking protocol to verify data integrity.

Identified methods form a comprehensive sample for enabling continuous, secure, and privacy-preserving auditing of cloud storage data integrity by third parties.

6 Conceptual Architecture

By analyzing extant literature on CA, interviewing auditors, providers and customers, an architecture for CA of cloud services was conceptualized (see Fig. 3) and will be described in the following.

6.1 Data Gathering

CA requires auditors to gather and assess comprehensive data sets on a regular basis. Interviews and workshops revealed that (external) third party access to audit-relevant data, and therefore auditors' data gathering capabilities, are limited due to technical, organizational, and legal reasons. First, technical limitations and barriers might hamper auditors to gather necessary auditing information by themselves. Integration of additional monitoring systems, matching auditees' heterogonous data formats and legacy systems, requires extensive modifications to auditees' systems, which can be quite expensive to implement, especially post hoc. More importantly, most service providers are not necessarily willing or obligated and may be even resisting to integrate auditors' techniques into their systems. Second, efficient data gathering and monitoring requires extensive knowledge about organizational processes, structures, system architectures; nonetheless an auditor's knowledge about an auditee's system and processes is limited due to the nature of focusing on potential security problems and her independence. Likewise, auditors are hesitant to externally interfere with auditees' systems to prevent security vulnerabilities. Third, due to legal requirements, gaining access to required data and systems might be limited for third party auditors as well.

To cope with these limitations, most audit-relevant information has to be gathered by the provider herself, and subsequently be made accessible for auditors—according to practitioners. Hence, performing continuous monitoring by service providers forms a prerequisite for the provision of audit-relevant data, and for auditors to perform efficient CA. Nonetheless, auditors can gather additional data by performing limited external CA.

6.1.1 Continuous Monitoring and Internal Auditing

Providers have already equipped their service centers with sophisticated monitoring technologies to gather service data and quickly detect malicious attacks, failures, and outages. Leveraging collected data for the purpose of CA as well is beneficial. Yet, participating in CA requires providers to use comprehensive *(continuous) monitoring systems* to ensure that all audit-relevant data is up-to-date, accurate, and available. Therefore, cloud providers should implement an extensive cloud logging framework as suggested by Ko et al. [32]. To adhere to CSC criteria presented in Section 4, 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 monitoring data across different systems, and to aggregate and anonymize (monitoring) data, and format data according to auditors' needs. Since auditing methodologies presented in Section 5 are mostly developed for internal auditing contexts, they can be implemented by service providers as well to gather audit-relevant data internally. For instance, by deploying internally a team of digital agents or implementing a monitoring and control layer, administrators can gather data across different cloud monitoring tools and store findings inside an *internal audit data mart*.

Gathering audit-relevant data by the service provider herself leads to several advantages compared to auditing that solely relies on external auditing. First, auditee resistance will decrease, and acceptance will increase when auditors do not interfere directly with auditees' systems. Second, providers' employees possess or can easily access required knowledge about internal processes and cloud systems. Third, audit-relevant data and information can be gathered and processed internally, hence, reducing security and privacy concerns. Fourth, instead of implementing standardized or inappropriate third party modules and software, an auditee can implement proprietary and customized internal auditing techniques aligned to their individual cloud architecture. However, a provider has to ensure that appropriate monitoring and internal auditing resources are allocated and integrated into daily operational management, and employee responsibilities are settled. Thus, providers have to adjust their organizational structures to meet CA prerequisites and criteria.

6.1.2 External Continuous Auditing

To gather additional audit-relevant data, auditors can perform limited external CA. In general, cloud components that are connected to the Internet can be (continuously) tested and scanned. Therefore, auditors should implement *continuous auditing systems*, comprising various auditing methods to perform (semi-)automated auditing processes for different scenarios. Hence, for example, performing penetration testing, external vulnerability scans, and using interceptor tools to analyze cloud systems, service availability, and encryption. Likewise, presented data integrity checks (see Section 5.5) can be performed externally. Further external assessments can be performed based on criteria requirements. For example, assuring that a *'security incident handling team has to be available 24 h, seven days a week'* by performing automated telephone calls or automatically sending predefined troubleshooting tickets and assessing responses. Moreover, auditors have to implement *systems to support audit planning, management and scheduling* to coordinate CA processes and to enable fluent and automated execution of auditing functions.

Practitioners empathized that implementation of foreign auditing components is limited but might be applicable in some cases. For example, a provider can implement a foreign component (e.g., EAM or digital agent), which requires solely minimal access privileges and only analyses non-confidential data. Therefrom, auditors might extract additional audit-relevant information from cloud services.

6.2 Data Exchange

Besides gathering data, providers have to manage a provision of audit-relevant information to ensure ongoing data exchange with auditors. Therefore, service providers need to establish an *internal auditing department*, which manages and supervises the gathering, processing, provision and transmission of audit-relevant information. This internal auditing department forms a linkage between provider and auditor when performing CA.

Practitioners suggest different data exchange approaches to assess ongoing certification adherence. First, providers might incorporate defined *data provision interfaces* to enable auditors accessing relevant data. Different types of data provision interfaces might be implemented, for example, a user interface (i.e., a simple web frontend presenting audit-relevant data) or a standardized application programming interface (i.e., XML, JSON, or Perl interfaces). On the other hand, auditors might offer *data exchange interfaces*, for instance, a *web interface* to upload or to enter auditees' data or to inform auditors about major changes. Second, auditees might transmit monitoring logs or exported data from existing monitoring systems (e.g., *Nagios*) to auditors. Finally, auditors might request auditees to provide reports according to defined frequencies. For example, when validating adherence to the exemplary criterion '*a provider should regularly perform reviews of firewall rules*', then an auditee can upload a short report that comprises various information, for instance, date, firewall policy version, number of offending firewall rules, initiated operations, and changes made.

6.3 Data Analysis and Presentation

Since data is provided on a high frequency, data should be stored by auditors in an *audit data mart* to enable automated data analysis. Therefrom, auditors should implement suitable *decision support systems* to improve audit and analyses efficiency, expedite decision-making processes, and to cope with potential alarm floods. DSS can be used to aggregate gathered information as well as efficiently and automatically decide to take actions or to alert auditors. Furthermore, these DSS might trigger additional auditing operations based upon external changes, for instance, announcement of new viruses or software vulnerabilities (e.g., *Heartbleed vulnerability*). Nonetheless, customers demand that auditors should manually validate auditing results on at least regular basis to ensure that results are not falsified due to technical errors.

Interviewees put high emphasize on customer enlightenment when performing CA to counteract customers' fear of loss of controls and to counteract the impression of using a black box when provisioning cloud services. Therefore, it is important to continuously publish auditing information to prove ongoing certification adherence and to increase transparency about cloud services. A fully transparent CA process is especially demanded by customers to increase trustworthiness. Practitioners recommend providing a user interface (e.g., a *web frontend for customers*) to inform customers about performing CA processes and ongoing certification (non-)adherence. In addition, they recommend informing customers about how and when data was gathered and analyzed to increase comprehensibility and accountability. More importantly, in cases of critical certification violations or major security incidents, customers should be automatically informed by auditors. Customers demand auditors to send periodic auditing reports that comprise a summary of performed auditing processes and suspicious incidents. Further on, customers should be able to configure frontends according to their needs, for example, choosing displayed criteria and type of graphical representation (e.g., chart or graph). Likewise, customers might be provided with functions to request renewed auditing, or to report identified issues or reasons for criteria non-adherence. Auditors might implement these functions as web services, requiring customers to pay an invocation fee (i.e., see [11]). Finally, auditing results should be archived for certain periods since auditors as well as customers are interested in comparing current with past data. For example, customers might want to look up data of the last month to check for CSC criteria adherence. For data analysis purposes, comparison of current data with historic data can aid the auditing service to learn and configure exceptions and alert patterns (e.g., rule-based configurations based on deviations from historic data).

6.4 Continuous Process Adjustments

The process of CA has to be continuously adjusted to cope with dynamics of an ever-changing and hostile environment. On the one hand, emerging environmental threats or changes in legal and regulatory landscape might induce auditors to adjust their auditing scope, for example, by adding new certification criteria. On the other hand, architectural changes of cloud services (e.g., adding new service functionalities) can cause providers and auditors to adjust their monitoring and auditing processes. Therefore, providers might incorporate the concept of CA into their change management processes to inform auditors on major changes.

7 Challenges

Discussion with practitioners revealed that major challenges have to be tackled before the proposed architecture can be applied in practice.

7.1 Risk of Audit-Data Manipulation

Provision of audit-relevant data by a provider herself has one challenging drawback: the risk of data manipulation. Providers might modify provided data to assure ongoing certification adherence. Preventing cloud service providers to manipulate or euphemize audit-relevant data is an important prerequisite to ensure that CA is trustworthy and reliable. Consequently, providers have to establish secure logging mechanisms which achieve a high degree of log integrity and confidentiality. In order to achieve this, we can build on findings from research area of cloud forensics. Cloud forensics is defined as the application of scientific principles, technological practices to reconstruct past cloud computing events through identification, collection, preservation, examination, interpretation, and reporting of digital evidence [70].

Researchers have proposed various procedures to deal with challenges of cloud forensics (i.e., malicious cloud service providers manipulating log files), ultimately enabling third party investigators to collect and analyze relevant data [71]. Cloud service provider can implement appropriate log adapters to extract and transfer log entries from different logging sources (e.g., hypervisor) to a central logging component [72]. This central logging component transforms log entries into a secure, encrypted and uniform log type. To prevent internal log manipulation, a trusted third party module (e.g., hardware or virtual module [71]) can be implemented that provides secure log encryption functions. Similar, various schemes are proposed (i.e., homomorphic encryption) and evaluated using open-source cloud computing platforms to ensure privacy and confidentiality of log data [73], [74].

Further on, one way of revealing data manipulation is to establish a chain of custody for digital evidence [75], which represents a roadmap that shows how data was collected, analyzed, and preserved in order to be presented as evidence in court. Moreover, several procedures are recommended to gather trusted audit-relevant data, including remote data acquisition over trusted and secure channels, usage of management planes, preforming live forensics on systems in running state, as well as snapshotting a clone of a virtual image among others (cf., [71] for a detailed comparison). Nonetheless, cloud forensics procedures will vary according to service and deployment model of cloud computing [74]. For example, Software- and Platform-as-a-Service models inherit very limited control over process or network monitoring, whereas in Infrastructure-as-a-Service settings some forensic friendly logging mechanism might be deployed. Future research should evaluate how existing procedures from cloud forensics research can be applied to enable CA.

Workshop participants and customers assessed a low likelihood of internal modification since continuous modification constitutes high expenditures. In addition, data manipulation requires a provider to store data volume twice; first unmodified data for internal evaluations, second modified data for auditors and customers. Finally, customers might reveal tampered data when using the service (e.g., tampered availability rate). Yet, customers as well as providers recommend that auditors should randomly perform validation tests on regularly basis to prevent data manipulation or reveal tampered data.

7.2 Security Challenges

Providers and auditors have to face several security challenges when providing and transmitting audit-relevant data, including protection of deployed (data exchange) interfaces, authorization of third parties, security of data transmission, and user interfaces as well as achieving high levels of data integrity and confidentiality. Moreover, auditors form a high valuable target for attackers since they receive data from different and mostly large-sized cloud service providers (due to high costs of CA).

7.2.1 Confidentiality Issues

Assuring confidentiality refers to preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information [76]. When data is transferred to auditors or presented to customers, privacy of audit-relevant data has to be ensured to prevent leakage of sensitive or security-relevant information. Therefore, data must be anonymized or filtered respectively. In this sense, providers have to precisely differentiate system monitoring data and cloud customers' data. Revealing sensitive customer data might breach service level agreements and consequently lead to financial compensation. Moreover, exchange of relevant data through using interfaces require providers or auditors to implement robust and secure access control systems and encryption mechanisms for data transmission. Attackers might perform brute force or man-in-the-middle attacks to retrieve sensitive data. Finally, providing sensitive cloud service data bears the risk of malicious auditors, who might abuse audit-relevant data. Therefore, auditors have to prove that data is kept confidential.

7.2.2 Integrity Issues

Providing integrity refers to guarding information against improper modification or destruction and includes ensuring information nonrepudiation and authenticity [76]. In the context of CA, ensuring integrity and guarding information against improper modification by external as well as internal subjects have to be considered. Attackers might be interested in targeting interfaces and frontends to modify provisioned and presented data. A modification of data might affect an auditor's assessment of criteria adherence, and thus might result in certification non-adherence or customer dissatisfaction. Likewise, attackers might tamper data, which is presented to customers to indicate bad service behavior. Ultimately, these attack scenarios can lead to loss of reputation or cancelation of contracts. Subsequently, providers and auditors need to achieve a high integrity of information and establish security mechanisms.

7.2.3 Availability Issues

Ensuring availability refers to ensuring timely and reliable access to and use of information [76]. In the context of CA, availability of cloud systems and provided interfaces has to be ensured. First, performing continuous monitoring and auditing process (e.g., ongoing data gathering, analysis and aggregation operations) might have a substantial performance impact on cloud services. Likewise, failures in these operations might lead to disturbance of cloud service operation. Hence, CA might threaten cloud service availability. Second, when audit-relevant data is provided via defined interfaces, providers have to assure availability of them. Attackers might target interfaces, for example, by performing distributed denial of service attacks to disturb the process of CA. In worst cases, this might lead to non-adherence of CSC criteria, since auditors are lacking corresponding audit information. Finally, providers have to assure that provided user interfaces for customers are available.

7.3 Automation & Cloud Service Individualism

Performing CA requires a high degree of automation. Yet, current CSC are mostly based upon manual auditing operations, for example, performing interviews and manual security tests as well as analyzing service and architecture documentations. Automation of these operations require a strong formalization, which is currently not achievable for every process [42]. Human auditors still need to manually validate specific criteria because some weaknesses might remain unrecognized on automated validation systems. Further on, research suggests that such an automation of 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 [77].

In addition, CA requires auditors to automatically assess comprehensive audit-relevant data. However, 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. Thus, for example, data logs are in heterogeneous formats and hence, it is difficult to automatically examine and analyze log evidence. Therefrom, auditors need to adjust their auditing and analysis methodologies based on context and capabilities of an auditee, which in turn hampers automation of auditing processes.

To deal with this individualism, auditors should develop a comprehensive metric and key performance indicator collection (see for example [17]), which can be used to evaluate criteria adherence based on different data inputs. Metrics might be derived and classified according the goal question metric method in a systematic top-down fashion by defining the goal to analyze cloud computing system designs and questions that help achieving corresponding goals [78]. Subsequently, auditors need to implement flexible and standardized auditing systems, which allow them to easily integrate or exclude providers since they might concurrently audit a broad variety of different cloud service providers. Notwithstanding these adjustments to cope with individualisms, auditors have to ensure that comparability between certification results is guaranteed.

8 Benefits

Providers as well as auditors must be motivated to participate in CA, and hence, to enable diffusion of continuous cloud service auditing. To motivate them, perceived benefits must be higher than perceived expenditures. Notwithstanding preceding challenges, CA will bear great benefits for auditors, providers and cloud customers [79].

Auditors can improve their audit efficiency by reducing auditing time and errors due to automated auditing process. 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. CA allows auditors to actively detect and investigate exceptions as they occur rather than to react after exceptions have long occurred. 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, CA can improve trustworthiness of auditors' CSC. Finally, auditors can counteract lack of cloud customers' control in CC environments by increasing transparency regarding operations of service providers.

Cloud service providers can benefit by participating in CA as well. First, internal processes and systems can be improved by implementing suitable monitoring and internal auditing techniques, and evaluating continuous feedback about how they are performing. In addition, providers receive ongoing expert assessments about their systems. Therefrom, CA positively effects service and risk management of providers, which was also emphasized by practitioners. Second, 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. Finally, providers can differentiate themselves in the cloud market by making their cloud services more transparent to customers. Thus, they may gain competitive advantages.

Cloud service customers can benefit when CA is performed. Typically, cloud environments are characterized by a lack of control since cloud customers cedes governance to cloud service providers. Especially when storing data in the cloud, customers fear that data could be compromised or leaked since they are lacking transparency about how and where data is stored and processed. CA can counteract this lack of control by increasing transparency regarding operations of providers. Through an increased transparency, CA ultimately tries to increase trustworthiness of customers in cloud services.

9 Conclusion

The ever-changing cloud environment, fast update cycles, and the increasing adoption of business-critical applications from cloud service providers demand for highly reliable cloud services. Continuously auditing such cloud services can assure a high level of security and reliability to (potential) cloud service adopters. However, methodologies to efficiently and continuously audit cloud services are still in their infancy. With our study, a first step to increase trustworthiness of CSC is provided by conceptualizing an architecture to continuously audit cloud services.

9.1 Contribution to Knowledge and Practice

Our findings reveal that various CSC criteria should be continuously audited to assure ongoing certification adherence and to prove secure and reliable services. Interviews revealed that most of existing methodologies are not applicable for third party service auditing purposes. Therefore, providers have to establish an internal auditing department, which provides audit-relevant data to auditors via defined and secure interfaces. Our conceptual architecture highlights important components (i.e., data provision and exchange interfaces, audit management modules, and customer frontends) as well as processes (e.g., sending reports, inform about major cloud changes, adjusting processes) that have to be implemented. These findings are relevant for practitioners and researchers.

We support auditors by providing a checklist (see Appendix B, available in the online supplementary material), which enables them to classify whether or not a high frequency auditing of CSC criteria is required, after the initial certification process is accomplished. Therefrom, auditors might start to verify criteria adherence on a higher frequency compared to current practices. Further on, we illustrate methodologies, which might be used by auditors to perform external auditing of cloud services (e.g., validating data integrity). Likewise, cloud service providers might implement presented auditing methods to set up an internal auditing department. By providing a first conceptual architecture, comprising important components to enable CA, we want to encourage auditors to implement CA techniques to create trustworthy certifications as well as practitioners to develop business models, for instance, auditing as a service in these contexts.

We also transferred the concept of CA in a new context, and discussed challenges and benefits of CA of cloud services. By identifying and assessing applicability of existing CA methodologies and conceptualizing an architecture, we identify gaps and means to perform CA of cloud services, hence forming a basis for future research. We want to encourage further researchers to address these issues, and thereby, ultimately create continuously secure and reliable cloud services.

9.2 Limitations

Nevertheless, this study has some limitations. First, even if we derived our architecture based on interviews with various providers, auditors and customers from different organizations, our evaluation regarding applicability of identified CA methodologies might be slightly biased since we evaluated applicability within three interviews with practitioners from one cloud service auditor only. Second, within our conceptual architecture, we do not provide any technical implementation. Instead, we focus on giving a broad outline and insights into current state and issues of CA to motivate researchers and practitioners to engage in these topics. We believe that CA of cloud services is one possible way to address current gaps and issues in CC. It is a step forward to a more trustworthy and transparent CC computing environment.

9.3 Future Research

As the discussion of challenges reveals, there is still plenty of research to do. Further research should focus on developing auditing methodologies adjusted to the CC context, especially concerning validation of security measures and adherence to critical cloud service characteristics (e.g., availability and scalability of services). Likewise, future research should examine how unique cloud computing characteristics influence (continuous) auditing practices. Identified methodologies need to be implemented to prove their practical and economic applicability in cloud environments. Therefore, identified and future methodologies need to be linked to CSC criteria and corresponding metrics to measure criteria adherence. Furthermore, research should focus on evaluations regarding acceptance and benefits of cloud providers when participating in CA as well as drivers and inhibitors for cloud service customers' demand for CA. Besides, future research should clarify how to manage certification violations, and if and how to inform cloud customers about certification (non-)adherence.

Acknowledgments

This research is funded by the German Federal Ministry for Education and Research (grant no. 16KIS0079).

References

[1] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011.

[2] K. M. Khan and Q. Malluhi, "Trust in Cloud Services: Providing More Controls to Clients," *Computer*, vol. 46, no. 7, pp. 94–96, 2013.

[3] S. Schneider and A. Sunyaev, "Determinant factors of cloud-sourcing decisions," *J. Inform. Techn.*, 2014.

[4] A. Sunyaev and S. Schneider, "Cloud services certification," *Commun. ACM*, vol. 56, no. 2, pp. 33–36, 2013.

[5] S. Cimato, E. Damiani, R. Menicocci, and F. Zavatarelli, "Towards the certification of cloud services," in *Proc. 9th World Congress Serv.*, Santa Clara, CA, USA, 2013, pp. 100–105.

[6] I. Windhorst and A. Sunyaev, "Dynamic certification of cloud services," in *Proc. 8th Int. Conf. Availability, Reliability Security*, Regensburg, Germany, 2013, pp. 412–417.

[7] S. M. Groomer and U. S. Murthy, "Continuous auditing of database applications," *Inf. Syst. J.*, vol. 3, no. 2, 1989.

[8] M. A. Vasarhelyi and F. B. Halper, "The continuous audit of online systems," *Auditing*, vol. 10, no. 1, pp. 110–125, 1991.

[9] B. Wang, B. Li, and H. Li, "Oruta," *IEEE Trans. Cloud Comput.*, vol. 2, no. 1, pp. 43–56, 2014.

[10] P. Massonet, S. Naqvi, C. Ponsard, J. Latanicki, B. Rochwerger, and M. Villari, "A monitoring and audit logging architecture for data location compliance in federated cloud infrastructures," in *Proc. IEEE Int. Symp. Parallel Distrib. Process. Workshops Phd Forum*, Shanghai,China, 2011, pp. 1510–1517.

[11] F. Doelitzscher, C. Reich, M. Knahl, A. Passfall, and N. Clarke, "An agent based business aware incident detection system for cloud environments," *J. Cloud Comput.*, vol. 1, no. 1, p. 9, 2012.

[12] S. Lins, S. Thiebes, S. Schneider, and A. Sunyaev, "What is really going on at your cloud service provider?," in *Proc. 48th Hawaii Int. Conf. Syst. Sci.*, 2015, pp. 1–10.

[13] P. Mell and T. Grance, "The NIST definition of cloud computing," 2011.

[14] S. Pearson, "Toward Accountability in the Cloud," *IEEE Internet Comput.*, vol. 15, no. 4, pp. 64–69, 2011.

[15] International Organization for Standardization, Conformity Assessment – Vocabulary and general principles, 17000:2004.

[16] S. Schneider, J. Lansing, F. Gao, and A. Sunyaev, "A taxonomic perspective on certification schemes," in *Proc. 47th Hawaii Int. Conf. Syst. Sci.*, Big Island, Hawaii, USA, 2014, pp. 1–10.

[17] P. Stephanow and N. Fallenbeck, "Towards continuous certification of Infrastructure-as-a-service using low-level metrics," in *Proc. 12th IEEE Int. Conf. Adv. Trusted Comput.*, Beijing, China, 2015, pp. 1–8.

[18] CICA/AICPA, "Continuous auditing," 1999.

[19] C. E. Brown, J. A. Wong, and A. A. Baldwin, "A review and analysis of the existing research streams in continuous auditing," *J. Emerging Technol. Account.*, vol. 4, no. 1, pp. 1–28, 2007.

[20] M. A. Vasarhelyi, M. Alles, S. Kuenkaikaew, and J. Littley, "The acceptance and adoption of continuous auditing by internal auditors," *Methodol. J. AIS Res.*, vol. 13, no. 3, pp. 267–281, 2012.

[21] J. Woodroof and D. Searcy, "Continuous audit implications of internet technology," in *Proc. 34th Annu. Hawaii Int. Conf. Syst. Sci.*, Island of Maui, HI, US, 2001, pp. 1–8.

[22] K. Singh, P. J. Best, M. Bojilov, and C. Blunt, "Continuous auditing and continuous monitoring in ERP environments," *Inf. Syst. J.*, vol. 28, no. 1, pp. 287–310, 2013.

[23] J. R. Kuhn Jr, and S. G. Sutton, "Continuous auditing in ERP system environments," *Inf. Syst. J.*, vol. 24, no. 1, pp. 91–112, 2010.

[24] C.-C. Lin, F. Lin, and D. Liang, "An analysis of using state of the art technologies to implement real-time continuous assurance," in *Proc. 6th World Congress Serv.*, Miami, FL, USA, 2010, pp. 415–422.

[25] M. A. Vasarhelyi, M. G. Alles, A. Kogan, and D. O'Leary, "Principles of analytic monitoring for continuous assurance," *J. Emerging Technol. Accounting*, vol. 1, pp. 1–21, 2004.

[26] C.-H. Yeh, T.-P. Chang, and W.-C. Shen, "Developing continuous audit and integrating information technology in e-business," in *Proc. IEEE Asia-Pac. Serv. Comput. Conf.*, Yilan, Taiwan, 2008, pp. 1013–1018.

[27] U. S. Murthy and S. M. Groomer, "A continuous auditing web services model for XML-based accounting systems," *Int. J. Account. Inform. Syst.*, vol. 5, no. 2, pp. 139–163, 2004.

[28] S. Lamparter, S. Luckner, and S. Mutschler, "Formal specification of web service contracts for automated contracting and monitoring," in *Proc. Hawaii Int. Conf. Syst. Sci.*, Waikoloa, Hawaii, 2007, pp. 1–10.

[29] C. Ardagna, E. Damiani, R. Jhawar, and V. Piuri, "A model-based approach to reliability certification of services," in *Proc. 6th IEEE Int. Conf. Digital Ecosyst. Technol.*, Italy, 2012, pp. 1–6.

[30] P. Stephanow, C. Banse, and J. Schütte, "Generating threat profiles for cloud service certification systems," in *Proc. 17th IEEE High Assurance Syst. Eng. Symp.*, 2016, pp. 1–8.

[31] P. Stephanow and M. Gall, "Language classes for cloud service certification systems," in *IEEE 11th World Congress Serv.*, 2015, pp. 127–134.

[32] R. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "TrustCloud," in *Proc. IEEE World Congress Serv.*, Washington, DC, USA, 2011, pp. 584–588.

[33] P. Mell, D. Waltermire, L. Feldman, H. Booth, A. Ouyang, Z. Ragland, and T. McBride, "CAESARS framework extension," 2012.

[34] M. D. Myers, *Qualitative Research in Business & Management*, 2nd ed. London, UK: SAGE, 2013.

[35] C. L.-Y. Chou, T. Du, and V. S. Lai, "Continuous auditing with a multi-agent system," *Decision Support Syst.*, vol. 42, no. 4, pp. 2274–2292, 2007.

[36] A. Ahmi and S. Kent, "The utilisation of generalized audit software by external auditors," *Managerial Audit. J.*, vol. 28, no. 2, pp. 88–113, 2012.

[37] T. Singleton and D. L. Flesher, "A 25 year retrospective on the IIA's SAC projects," *Managerial Audit. J.*, vol. 18, no. 1, pp. 39–53, 2003.

[38] N. Mahzan and A. Lymer, "Examining the adoption of computer-assisted audit tools and techniques," *Managerial Audit. J.*, vol. 29, no. 4, pp. 327–349, 2014.

[39] I. Pedrosa and C. J. Costa, "New trends on CAATTs," in *Proc. Int. Conf. Inform. Syst. Des. Commun.*, Lisboa, Portugal, 2014, pp. 138–142.

[40] J. Gao, "Technical framework model of continuous online assurance," in *Proc. Int. Conf. E-Business E-Government*, Guangzhou, China, 2010, pp. 2141–2144.

[41] G. Koschorreck, "Automated audit of compliance and security controls," in *Proc. 6th Int. Conf. IT Security Incident Manage. IT Forensics*, Stuttgart, Germany, 2011, pp. 137–148.

[42] M. Alles, G. Brennan, A. Kogan, and M. A. Vasarhelyi, "Continuous monitoring of business process controls," *Int. J. Account. Inform. Syst.*, vol. 7, no. 2, pp. 137–161, 2006.

[43] Y. Chen, "Continuous auditing using a strategic-systems approach," *Internal Auditing*, vol. 19, no. 3, pp. 31–36, 2004.

[44] B. Schroeder, "On-line monitoring," *Computer*, vol. 28, no. 6, pp. 72–78, 1995.

[45] Z. Rezaee, A. Sharbatoghlie, R. Elam, and P. L. McMickle, "Continuous auditing," *Auditing*, vol. 21, no. 1, pp. 147–163, 2002.

[46] J. E. Hunton and J. M. Rose, "21st Century Auditing," *Account. Horizons*, vol. 24, no. 2, pp. 297–312, 2010.

[47] R. L. Braun and H. E. Davis, "Computer-assisted audit tools and techniques: analysis and perspectives," *Managerial Audit. J.*, vol. 18, no. 9, pp. 725–731, 2003.

[48] A. Fuggetta, G. Picco, and G. Vigna, "Understanding code mobility," *IEEE Trans. Softw. Eng.*, vol. 24, no. 5, pp. 342–361, May 1998.

[49] J. M. Shaikh, "E-commerce impact," *Managerial Audit. J.*, vol. 20, no. 4, pp. 408–421, 2005.

[50] T. C. Du, E. Y. Li, and E. Wei, "Mobile agents for a brokering service in the electronic marketplace," *Decision Support Syst.*, vol. 39, no. 3, pp. 371–383, 2005.

[51] H. Ye, J. Yang, and Y. Gan, "Research on continuous auditing based on multi-agent and web services," in *Proc. Int. Conf. Manage. e-Commerce e-Government*, Beijing, China, 2012, pp. 220–225.

[52] J. Zhang and C. Wan, "Securing continuous auditing in wireless network," in *Proc. Int. Conf. E-Business E-Government* , Shanghai, China, 2011, pp. 1–4.

[53] C.-L. Fang, D. Liang, F. Lin, C.-C. Lin, and W.-C. Chu, "A portable interceptor mechanism on SOAP for continuous audit," in *Proc. Asia Pac. Softw. Eng. Conf.*, Bangalore, India, 2006, pp. 95–104.

[54] D. Żmuda, M. Psiuk, and K. Zieliński, "Dynamic monitoring framework for the SOA execution environment," *Proc. Comput. Sci.*, pp. 125–133, 2010.

[55] C.-T. Kuo, H.-M. Ruan, C.-L. Lei, and S.-J. Chen, "A mechanism on risk analysis of information security with dynamic assessment," in *Proc. 3rd Int. Conf. Intell. Netw. Collaborative Syst.*, Fukuoka, Japan, 2011, pp. 643–646.

[56] M. Jans, M. Alles, and M. Vasarhelyi, "The case for process mining in auditing," *Methodol. AIS Res.*, vol. 14, no. 1, pp. 1–20, 2013.

[57] Q. Fu, J.-G. Lou, Y. Wang, and J. Li, "Execution anomaly detection in distributed systems through unstructured log analysis," in *Proc. Int. Conf. Data Mining*, Miami, FL, USA, 2009, pp. 149–158.

[58] H. Du and S. Roohani, "Meeting challenges and expectations of continuous auditing in the context of independent audits of financial statements," *Int. J. Audit.*, vol. 11, no. 2, pp. 133–146, 2007.

[59] J. L. Perols and U. S. Murthy, "Information fusion in continuous assurance," *Inf. Syst. J.*, vol. 26, no. 2, pp. 35–52, 2012.

[60] C.-H. Wu, Y. E. Shao, B.-Y. Ho, and T.-Y. Chang, "On an agent-based architecture for collaborative continuous auditing," in *Proc. 12th Int. Conf. Comput. Supported Cooperative Work Des.*, Xi'an, China, 2008, pp. 355–360.

[61] Z. M. Jiang, A. Hassan, P. Flora, and G. Hamann, "Abstracting execution logs to execution events for enterprise applications," in *Proc. 8th Int. Conf. Quality Softw.*, Oxford, England, 2008, pp. 181–186.

[62] R. Accorsi, “Automated privacy audits to complement the notion of control for identity management,” 2007.

[63] R. Accorsi and T. Stocker, “Automated privacy audits based on pruning of log data,” in *Proc. 12th Conf. Enterprise Distrib. Object Comput.*, Munich, Germany, 2008, pp. 175–182.

[64] R. Nithiavathy, “Data integrity and data dynamics with secure storage service in cloud,” in *Proc. Int. Conf. Pattern Recog., Inform. Mobile Eng.*, Salem, Germany, 2013, pp. 125–130.

[65] K. Yang and X. Jia, “An efficient and secure dynamic auditing protocol for data storage in cloud computing,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 9, pp. 1717–1726, Sep. 2013.

[66] Y. Zhu, G.-J. Ahn, H. Hu, S. Yau, H. An, and C.-J. Hu, “Dynamic audit services for outsourced storages in clouds,” *IEEE Trans. Serv. Comput.*, vol. 6, no. 2, pp. 227–238, Apr.–Jun. 2013.

[67] C. Liu, J. Chen, L. Yang, X. Zhang, C. Yang, R. Ranjan, and K. Ramamohanarao, “Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 9, pp. 2234–2244, Sep. 2014.

[68] B. Wang, B. Li, and H. Li, “Knox” in *Proc. Appl. Cryptograph. Netw. Security*, 2012, pp. 507–525.

[69] H. C. H. Chen and P. P. C. Lee, “Enabling data integrity protection in regenerating-coding-based cloud storage,” *IEEE Trans. Parallel Distrib. Syst*, vol. 25, no. 2, pp. 407–416, Feb. 2014.

[70] National Institute of Standards and Technology, NIST Cloud Computing Forensic Science Challenges: *Draft NISTIR 8006*.

[71] A. Pichan, M. Lazarescu, and S. T. Soh, “Cloud forensics,” *Digital Investigation*, vol. 13, pp. 38–57, 2015.

[72] T. Kunz, P. Niehues, and U. Waldmann, “Technische unterstützung von audits bei cloud-betreibern,” *DuD*, vol. 37, no. 8, pp. 521–525, 2013.

[73] J. R. Rajalakshmi, M. Rathinraj, and M. Braveen, “Anonymizing log management process for secure logging in the cloud,” in *Proc. Int. Conf. Circuit, Power Comput. Technol.*, India, 2014, pp. 1559–1564.

[74] S. Zawoad, A. K. Dutta, and R. Hasan, “SecLaaS,” in *Proc. 8th ACM SIGSAC Symp. Inform., Comput. Commun. Security*, Hangzhou, China, 2013, pp. 219–230.

[75] C.-H. Lin, C.-Y. Lee, and T.-W. Wu, “A cloud-aided RSA signature scheme for sealing and storing the digital evidences in computer forensics,” *Int. J. Security Its Appl.*, no. 2, p. 241, 2012.

[76] National Institute of Standards and Technology, Federal Information Security Management Act of 2002.

[77] M. G. Alles, A. Kogan, and M. A. Vasarhelyi, “Audit automation for implementing continuous auditing,” 2008.

[78] M. Becker, S. Lehrig, and S. Becker, “Systematically deriving quality metrics for cloud computing systems,” in *Proc. 6th ACM/SPEC Int. Conf. Perform. Eng.*, Austin, TX, USA, 2015, pp. 169–174.

[79] S. Lins, P. Grochol, S. Schneider, and A. Sunyaev, “Dynamic certification of cloud services: Trust, but verify!,” in *Proc. IEEE Security and Privacy*, vol. 14, no. 2, forthcoming, 2016.

Sebastian Lins is a research assistant at the Department of Information Systems, University of Cologne, Germany. His main interests in the field of information systems research are the (dynamic) certification and continuous auditing of cloud services.

Stephan Schneider is a postdoctoral researcher at the Department of Information Systems, University of Cologne, Germany. His research focuses on strategic decision-making in cloud sourcing projects as well as on cloud security and certification of cloud computing infrastructures.

Ali Sunyaev is an assistant professor at the Department of Information Systems, University of Cologne, Germany. He has published several international journal articles in leading journals such as *Communications of the ACM*, *Journal of Information Technology and IEEE Software*.