Journal of Internet Services and Applications
a SpringerOpen Journal

RESEARCH Open Access

Adoption of security as a service

Christian Senk

Abstract

Security as a Service systems enable new opportunities to compose security infrastructures for information systems. However, to date there are no holistic insights about their adoption and relevant predictors. Based on existing technology acceptance models we developed an extended application-specific research model including formative and reflective measures. The model was estimated applying the *Partial Least Squares* technique to address the prediction-oriented nature of the study. A subsequent online survey revealed that a large number of industries shows significant and steadily growing interest in *Security as a Service*. Adoption drivers were investigated systematically.

Keywords: Cloud computing, Partial least squares, Security as a service

1 Introduction

Companies face an increasing threat regarding the security and safety of their information systems due to the opening of security domains for web-based access in the course of current technological developments such as *Federated Identity Management* [1] and *Cloud Computing* [2,3]. In this regard, *Cloud Computing* is a model "for enabling convenient, on-demand network access to a shared pool of configurable computing resources [...]" [4]. These resources are referred to as *Cloud services* and can logically be assigned to the infrastructure, (*Infrastructure as a Service*, IaaS), middleware (*Platform as a Service*, PaaS) or application software layer (*Software as a Service*, SaaS) [5,6]. The *Cloud Computing* model itself not only induces certain security-related risks, it also opens up new opportunities to obtain innovative security solutions in a technically and economically flexible way in order to cope with rising security demands [7]. The outsourcing of security according to SaaS principles is referred to as *Security as a Service* (SECaaS) [3,8]. Such systems are considered to be the next step in the evolution of *Managed Security Services* (MSS) and differ clearly from traditional outsourcing models or on-premises deployments [3,8,9]. According to GARTNER RESEARCH, the demand for SECaaS will grow significantly and might substantially change existing IT security infrastructure landscapes [10]. However, no deep insights about the current adoption and future developments exist. In this regard, based on an expert-group discussion[a] we defined that the answers to the following research questions (RQ) are important to predict the future of SECaaS:

- **RQ1:** Is there a market for SECaaS enterprise applications in general and for specific application types in particular?
- **RQ2:** Which are the key drivers and inhibitors for the adoption of SECaaS?
- **RQ3:** Which benefits are perceived to be relevant by potential adopters of SECaaS?
- **RQ4:** Which risks are perceived to be relevant by potential adopters of SECaaS?
- **RQ5:** Which organization-specific factors (e.g. company size) affect the acceptance of SECaaS?

The main objective of this paper is to answer these research questions through empirical research in order to gain insights valuable for both potential consumers and providers of SECaaS. The remainder of this paper is structured as follows: Section 2 defines SECaaS and overviews related work regarding the adoption of similar technologies. In Section 3 the research concept is specified and justified. Section 4 gives an overview of the results of the estimation of the research model and the related hypotheses. Afterward, the findings are discussed respecting the specified research questions. Section 5 concludes the paper.

Correspondence: christian.senk@wiwi.uni-regensburg.de
University of Regensburg, Regensburg, Germany

2 Theoretical background

This chapter provides the theoretical background for the context of the study. This includes the object of adoption (SECaaS), which is defined in Subsection 2.1. Subsequently, an overview of related work regarding the adoption of similar technological innovations is provided in Subsection 2.2 in order to identify adequate research approaches.

2.1 Security as a service

SECaaS is a service-oriented approach to IT security architecture and thus a consequent evolution of traditional security landscapes [8,9]. It is defined as a model for the delivery of standardized and comprehensive security functionality in accordance with the SaaS model [8,11]. It thus follows the *Cloud Computing* model. Hence, SECaaS systems are delivered in form of Cloud services complying with related principles. This excludes built-in security controls of existing Cloud services [11]. Key attributes of Cloud services contain the following [5,6,12]:

- Application and underlying infrastructure are abstracted and offered through service interfaces;
- Standardized network access by any device;
- Scalability and flexibility of the underlying infrastructure;
- Shared and multi-tenant resources;
- On-demand self-service provisioning and near real-time deployment;
- Flexible and fine grained pricing without up-front commitments.

Based on the market-oriented taxonomy of KARK for outsourced security services [13] and the adaption of SENK AND HOLZAPFEL [14] we classify SECaaS systems as depicted in Table 1. This classification scheme was recently validated by a survey of existing SECaaS offerings [14]. According to that survey, the majority of existing SECaaS products cover *Endpoint Security* or *Content Security* applications [14]. The authors further outline existing systems' deficient compliance with Cloud and SaaS design principles. Especially inflexible pricing models often restrict the potential value of existent SECaaS systems [14]. It has to be noted that the granularity of SECaaS offerings can vary from fine-grained basic services addressing highly specific security needs (e.g. biometric user authentication) to coarse-grained solutions covering a broad set of security functionalities.

The delivery of security services according to the SECaaS model differs clearly from traditional MSS provisioning and on-premises deployments (see Figure 1). *On-premises security systems* are deployed, operated, and maintained on the client's side [11]. This requires the allocation of dedicated IT and human resource capacities. Service costs do not scale up or down with the actual degree of capacity utilization. None of the identified Cloud principles apply [14]. *Managed Security Services* are characterized in that a dedicated security service instance is set up for a client organization by an external service provider. This involves the prior negotiation of individual *Service Level Agreements* (SLA) [11]. In this regard, the provider is responsible for the operation and maintenance of the system [15-17]. Such security services do not provide for native multi-tenancy. Hence, the instant service use is not feasible and economies of scale are not exhausted [18]. Additionally, service usage may involve the deployment of dedicated software and hardware components and due to the initial effort required clients are often bound to providers by fixed-term licenses and up-front commitments [19]. Traditional managed service provisioning thus follows the *Application Service Providing* (ASP) model [12,14,20]. In contrast, *Security as a Service* solutions are fully operated and maintained by the service provider with no dedicated client-sided hardware or software necessary [11,14]. Full virtualization of the security service ensures the highest degree of capacity utilization. This makes the service usage highly cost-effective to the customer and enables fine-grained pay-per-use models. A virtualized multi-tenancy architecture not only enables the instant start of service use but also leverages inherent data aggregation benefits for service providers [14]. Moreover, operational and organizational flexibility is improved [11].

2.2 Adoption of related technologies

The term *Adoption* can be traced back to ROGERS' (1962) diffusion of innovations theory and is defined as a consumer's positive decision to accept and use an innovation, which ultimately leads to a positive investment decision and actual use [21]. Adopters can be individuals or organizations [22].

There are only a few current insights regarding the adoption of the outsourcing of IT security. GARTNER and FORRESTER RESEARCH conducted analyses of the MSS market and forecasted a steady and significant growth [7,13]. Moreover, FORRESTER RESEARCH surveyed IT security decision makers and identified major benefits of MSS [13]: Quality improvements, 24×7 support, cost reduction, and decrease of the complexity of security infrastructures. However, the study is not suitable regarding the research questions identified in this paper since the adoption was not investigated holistically and not focused on Cloud systems.

Benlian et al. conducted a meta-survey of the adoption of SaaS systems and applied different research theories [23]. They concluded that behavioral theories reveal more consistent results regarding the adoption of SaaS systems

Table 1 Classification of SECaaS applications

Application type	Description
Application security	Secure operation of software applications (e.g. application firewalls, code analyzers)
Compliance & IT Security management (ITSM)	Support of the client organization's compliance and IT security management (e.g. automatic compliance checks, benchmarking)
Content security	Protection of content data from intended attacks and undesired events (e.g. e-mail encryption, filtering of network traffic)
Endpoint security	Protection of servers or client computers in networks (e.g. malware protection, host-based intrusion detection)
Identity & access management	Identification of users, provisioning of user identity attributes and assignment of necessary privileges (e.g. single sign-on, multi-factor authentication)
Devices management	Remote management of client-sided security systems (e.g. intrusion detection and prevention systems)
Security information & event management (SIEM)	Specific security-related functions for monitoring complex IT systems (e.g. archiving and analysis of log-data, forensic analysis)
Vulnerability & threat management (VTM)	Detection of threats apart of eminent internal security incidents (e.g. patch management, notifications on current attacks)

than economic or strategic research theories [23]. Behavioral theories include the *Technology Acceptance Model* (TAM) [24], the *Theory of the Diffusion of Innovation* [21], and the *Unified Theory of Acceptance and Use of Technology* (UTAUT) [22]. The results indicate that the adoption of SaaS technologies is mainly influenced by [23]:

- Social influences,
- Attitude toward the technology,
- Uncertainty of adoption,
- Strategic value of respective resources.

However, due to the underlying research design, these results do not provide for causality [23]. Benlian et al. also concluded that both the adoption and adoption drivers differ across application types, which should be considered in future research [23]. Previous research indicates a higher susceptibility to SaaS adoption for smaller and medium-sized companies [23] and a different perception of risks and potential benefits by large-scale organizations [25], although no correlation was discovered between company size and adoption [23]. Udoh applied a combined model including elements of UTAUT and TAM and observed that the adoption of grid, Cloud and related technologies can be causally explained by four predictors [26]:

- Effort expectations (Perceived ease of use),

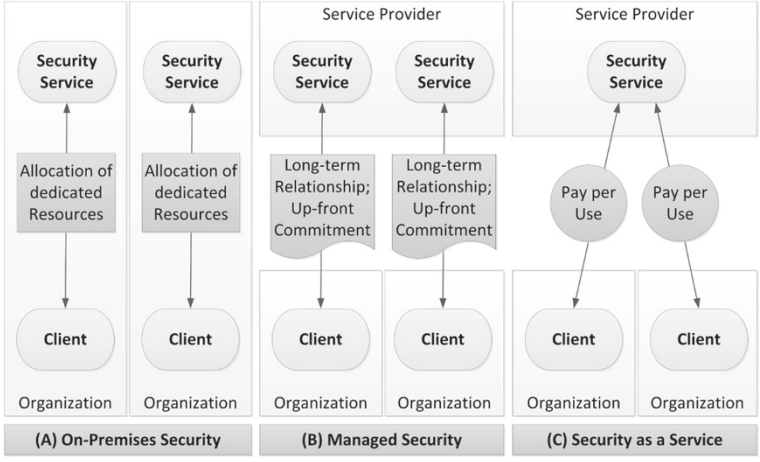

Figure 1 Security service delivery models.

- Risk expectations (Trust),
- Performance expectations (Perceived usefulness),
- Individual attitude.

Udoh's model provides a very high level of explanation which indicates a high aptitude for its application in similar technology acceptance studies [26]. Furthermore, its generic constructs can be itemized according to the specifics of subsequent research.

3 Research design

Based on related studies [23,26], this paper applies the *Structural Equations Modeling* methodology. For the model estimation involved, the *Partial Least Squares* technique is used. The methodology is introduced and justified in Subsection 3.1. Subsequently, in Subsection 3.2, a system of hypotheses -the research model- is developed. In Subsection 3.3, the measurement model is derived from this research model.

3.1 Methodology

Common technology acceptance theories like TAM or UTAUT are based on the development and testing of hypotheses regarding the influences of theoretical constructs on each other [22]. A system of hypotheses can be modeled as a system of equations [27]. A common approach to solving such systems is *Structural Equations Modeling* (SEM) [27]. SEM is defined as "a comprehensive statistical approach to testing hypotheses about relations among observed and latent variables" [27]. Besides the structural model, which primarily prescribes hypothetical relations between latent variables, a measurement model is required to quantize thes variables [27].

The measurement model prescribes not directly observed (latent) variables of the structural model by a set of measurable indicators [27]. Measurement models can be reflective or formative. Reflective measurement models assume empirically measurable variables. In this regard, the latent variable causes a set of reflective measurement indicators which correlate highly among each other [28]. In contrast, formative measurement models estimate a latent variable, applying a set of indicators, which are assumed to cause the construct [29]. This facilitates the differentiated analysis of the relevance and strength of certain influences on a theoretical construct [28]. Formative measures are mainly intended to explain the composition of a construct, whereas reflective measures only indicate a construct's outcome [28]. Therefore, on the one hand, formative measures lead to deeper practical insights than reflective ones and are more suitable for practical research applications [28]. On the other hand, such measurement models are restricted regarding the application of quality indicators [28]. To avoid this disadvantage, formative and reflective measures can be combined to form *Multiple Indicators, Multiple Causes* (MIMIC) models [28].

To estimate the comprehensive model either covariance-based approaches (CB-SEM) or the variance-based *Partial Least Squares* (PLS-SEM) technique can be applied [30]. Both approaches provide different benefits and drawbacks that imply their qualification for specific applications in research [28,30]. The PLS-SEM technique is more suitable for the research for this study due to four reasons: (1) the prediction-oriented research goal to explain the adoption of SECaaS (dependent variable) as comprehensively as possible; (2) the formative measurement of perceived overall risks and benefits which is required to get a deep and differentiated understanding of the composition of relevant adoption drivers; (3) the small sample size expected relative to the high complexity of the research model implied by the high number of hypothesized influences; (4) the possibility of applying fewer than four indicators for latent variables which is necessary to keep the study's questionnaire as purposive as possible [28].

The model estimation was performed using the software *SmartPLS* developed by Ringle et al. [31]. The tool facilitates the building of both structural and measurement models and was successfully applied in similar studies [32]. Further quality metrics were calculated using the statistics software *SPSS PASW Statistics*[b].

3.2 Research model

In SEM, hypotheses are relationships between latent variables which are represented by the structural model [27,28]. The system of hypotheses must be theoretically well-grounded [28]. This was assured since its development was based on related literature in the fields of *Cloud Computing*, SaaS and MSS, and continuously validated by an expert group[c] (Below, this expert group is referred to as the *Expert Panel*) using a dedicated online discussion platform (*PBworks*[d]). The labels used for the study's constructs represent the essence of the construct and are assumed to be independent regarding their theorized content. Constructs and hypothesized influences are described and justified below.

3.2.1 Adoption

The endogenous variable `Adoption` depicts the degree to which a certain entity intends to use SECaaS. This includes both the plan for future deployment [22,26] and the present adoption by an organization [22]. In this regard, the behavioral intention to use a system and actual use can be modeled either separately or using a single construct [33]. We chose the second option to keep the model purposive. The measurement of this variable allows implications about the current state and future development of the SECaaS market. Thus, we utilize `Adoption` to cope

with RQ1. The variable was hypothesized to be driven by the general determinants for grid and Cloud adoption identified [26]. These address RQ2 and represent the first four hypotheses (H) of this study as depicted in Figure 2: `Adoption` is significantly influenced by `Perceived Ease of Use` (H1), `Perceived Usefulness` (H2), `Trust` (H3), and `Attitude` (H4).

3.2.2 Perceived ease of use

This variable is defined as the degree to which the adopter believes that applying SECaaS is effortless [22,26,34,35]. From a client organization's point of view this involves the integration in the IT security infrastructure [11,15] as well as the actual use of the system [36]. Cloud-based security systems promise high ease of use since service interfaces are based on standardized internet technologies and can be accessed ubiquitously via thin clients (e.g. web browsers) [14]. It is questionable whether this fact affects the adoption and whether it is reflected by the perception of the adopters.

3.2.3 Perceived usefulness

`Perceived Usefulness` is defined as the degree to which an organizational adopter believes that the application of SECaaS increases the performance of the organization [22,26,34,35]. Performance expectation is a key driver for adoption [22,34]. Based on related literature Benlian et al. identified five specific benefit dimensions for SaaS service consumers which are hypothesized for SECaaS according to RQ3 [25]:

- *Perceived Flexibility Benefits:* The SaaS model implies a low organizational dependence of service consumers on service providers. Therefore, switching barriers are low and strategic flexibility regarding IT and IT security architectures is increased [11,25]. Furthermore, service use can be adapted flexibly to actual quantitative and qualitative needs [25].
- *Improved Resource Access:* Low entry barriers enable easy access to specific resources, skills and technologies of the external service providers [15,25].

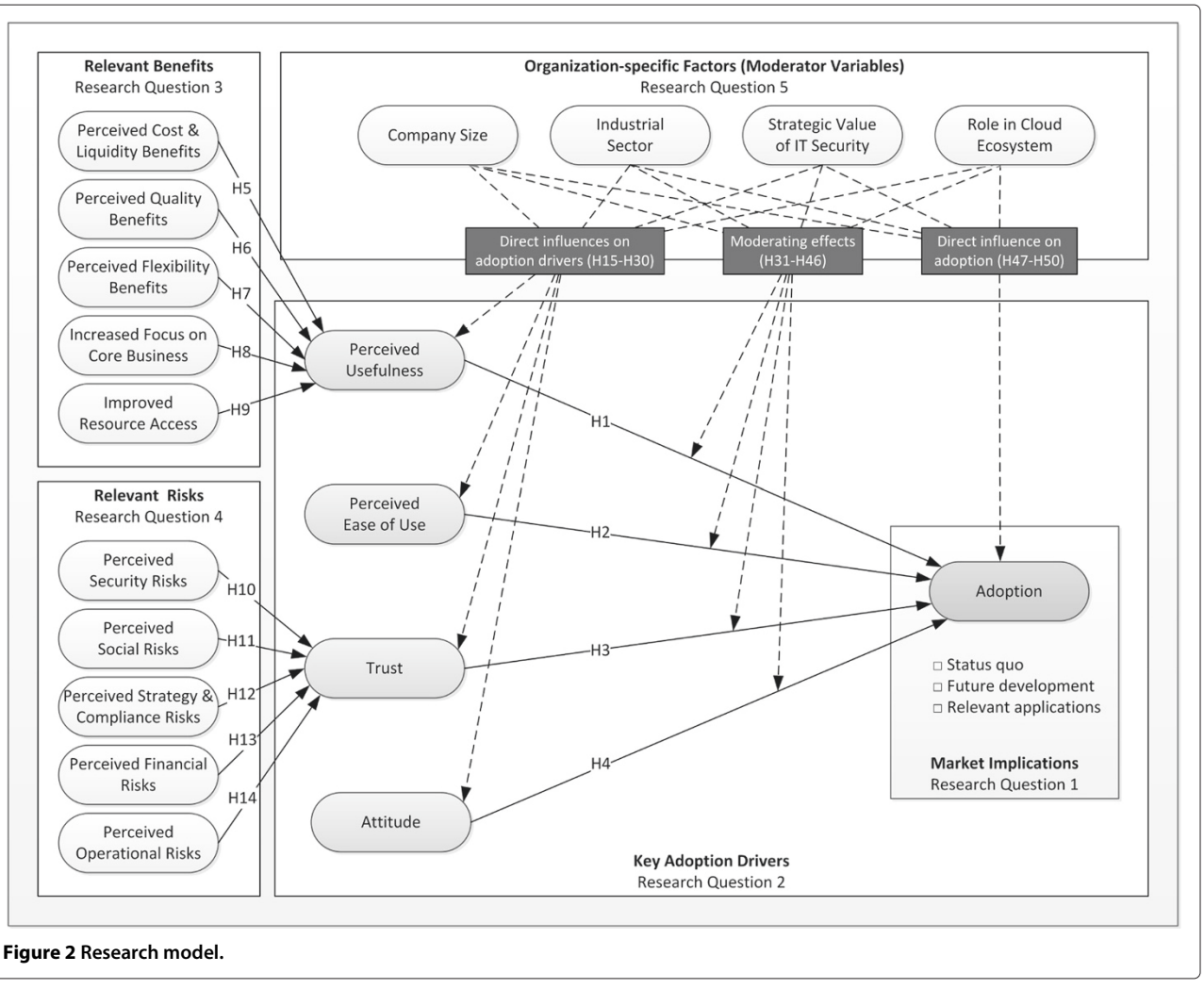

Figure 2 Research model.

Particularly mid-sized or smaller organizations might derive advantages from that when they cannot afford the time and effort involved in roviding sophisticated IT security resources on their own [11].

- *Perceived Cost & Liquidity Benefits:* Multi-tenancy architectures leverage economies of scale at the service providers' site. At the same time, service consumers' assumed low switching barriers induce a pricing pressure, forcing service providers to share respective savings. This ultimately leads to lower costs of operation and maintenance for service consumers [13,15,25]. Hence, on-demand pricing models enable decreased capital commitment [11,25]. Furthermore, the outsourcing model facilitates the transfer of financial risks of security incidents and thus the reduction of recovery costs [37].
- *Perceived Quality Benefits:* Security service providers use to be highly specialized, which implies their ability to provide a higher quality of service [11,13,15,16]. In addition, due to low switching barriers, service providers are forced to provide permanent high service quality [25]. Moreover, multi-tenancy architectures enable cross-client data aggregation and the application of business intelligence techniques [14]. Identified patterns can be used to improve quality of service, such as the performance of anti-virus applications, for instance. Lastly, SECaaS services are permanently up-to-date without the necessity of time-delayed updates at the client's site [11].
- *Improved Focus on Core Business:* The outsourcing of certain systems according to SaaS (or SECaaS) de-allocates internal resources [11,25]. These resources can be (re-)allocated to an organization's core business, which might increase overall performance [15,25] - assuming that IT security is not the core competency. Hence, this is also one of the major drivers for IT security outsourcing in general [38].

Many IT outsourcing programs do not yield expected performance outcomes [39,40]. Reasons include exaggerated expectations, poorly developed business cases, deficient change management, non-transparency of vendor performance, and lock-in effects [40]. This so-called "IT outsourcing paradox" [40] might affect the expected usefulness of SECaaS and its influence on the adoption.

3.2.4 Trust

The adoption of grid and Cloud systems is highly influenced by perceived risks [18,23,26,41,42]. This influence is represented by the variable `Trust`, which is interpreted as a semantic inversion of perceived risk. BENLIAN ET AL. identified SaaS-specific risk dimensions which are hypothesized in analogy to `Perceived Usefulness` addressing RQ4 [25]:

- *Perceived Security Risks:* The outsourcing of systems according to SaaS implies the loss of control over the processed data and requires the client organization to interface with the external service. This causes risks regarding the enterprise data and affected processes [11,15,25,42]. In this regard, Cloud-specific security risks focus on resource protection, communication and storage security, and authentication and authorization [2].
- *Perceived Social Risks:* The outsourcing of applications induces social risks including internal resistance or negative influences on the organization's image [25].
- *Perceived Strategy & Compliance Risks:* The outsourcing of certain systems might involve the loss of critical capabilities [25] and, in turn, the risk of an increased dependency on the service provider [15,37]. Furthermore, the service consumers might lose the control to ensure the compliance with legal and regulative requirements [15].
- *Perceived Financial Risks:* The deployment of SaaS services might involve unanticipated costs [25]. This includes the organization's own security infrastructure and service customization [11,15].
- *Perceived Operational Risks:* Since service operation is fully controlled externally there is the risk of the service provider not complying with existing SLAs. This might affect service quality, performance, and availability [15,25,42].

3.2.5 Attitude

The `Attitude` construct represents an adopter's individual positive or negative behavior toward an innovation and is considered to be independent from the othervariables [22,26,43]. It can be prescribed by individual preferences or perceived relative advantage to related technologies [22,26]. Its relevance for SaaS adoption is indicated by previous research [23].

3.2.6 Moderator variables

The validity of PLS-SEM results can be compromised by heterogeneous and conflicting data [30]. Potential sources for heterogeneity can be modeled and tested by means of moderator analyses [30]. Venkatesh et al. propose the use of moderators in addition to key determinants to account for dynamic influences and thus to improve the quality of adoption research models [22]. Moderators are variables that influence the relation between two constructs positively or negatively [22,28]. Moderators at the individual level include demographic characteristics and organizational context (e.g. gender, age) [22]. Since our

Table 2 Metrically measured indicators

Construct	Indicator(s)	Reference(s)
Adoption (refl.)	Actual use	[22,23,26]
	Use intent short-term (next 3 years)	
	Use intent mid-term (4–7 years)	
	Use intent long-term ($\geq$ 7 years)	
Adoption (form.)	Actual use/intent of Endpoint Security applications	[13,14,23]
	Actual use/intent of content security applications (appl.)	
	Actual use/intent of application security applications	
	Actual use/intent of compliance & IT security management appl.	
	Actual use/intent identity & access management appl.	
	Actual use/intent of managed devices applications	
	Actual use/intent of security information & event management appl.	
	Actual use/intent of threat & vulnerability management appl.	
Perceived ease of use (refl.)	General ease of use	[26,34]
	Ease of learning	
	Ease of target achievement	
Perceived ease of use (form.)	Ease of initial integration/deployment of the service	[13-15,36]
	Usability of the service	
	Ease of customizing the service	
	Comprehensive support by service provider	
Perceived usefulness (refl.)	Increase in performance	[26,34]
	General usefulness	
	Increase in effectiveness	
Perceived cost & liquidity benefits (form.)	Reduction in costs of operation and maintenance	[11,13-15,25,37]
	Variabilization of IT security costs	
	Reduction in recovery costs	
Perceived quality benefits (form.)	Transparency & control of security department	[11,13-16,25]
	Increase in organizational level of security	
	Improvement of legal and regulative compliance	
Perceived flexibility benefits (form.)	Flexibility of IT and security processes	[11,13,14,25]
	Flexibility of business processes	
	Reactivity regarding security-related problems	
Increased focus on core business (form.)	Decrease in employee errors	[11,13-15,25,37,38]
	Time savings in security management	
Improved resource access (form.)	Enablement of access to new technologies	[11,15,25]
	Access to external know-how	
	Independence from dedicated systems	
Trust (refl.)	Overall trust in adoption	[22,23,26]
	Trust in certified service providers	
	Hesitation due to uncertainty	
Perceived security risks (form.)	Vulnerability to unauthorized service access	[2,11,14]
	Deficient data mitigation and security	
	Vulnerability regarding network-based attacks	
	Deficient service continuity	

Table 2 Metrically measured indicators *(Continued)*

Perceived strategy & compliance risks (form.)	Dependence on service providers	[14,15,25,37]
	Inability to comply with obligations to produce supporting documents	
	Non-compliance with data protection regulations	
Perceived social risks (form.)	Internal resistance	[23,25]
	Loss of image	
Perceived financial & operational risks (form.)	Unexpected costs of integration	[11,15,25,42,45]
	Deficient provider's compliance with SLAs	
Attitude (refl.)	General attitude toward cloud technologies	[22,23,26]
	Relative advantage over managed security	
	Relative advantage over on-premises systems	
Strategic value of IT security (refl.)	Criticality of IT security for business	[23]

research focuses on adoption by organizational entities, we hypothesized new moderators to address RQ5. As part of the aforementioned expert workshop in the course of a session of the "IT security solutions" working group of the German Federal Association for Information Technology, Telecommunications and New Media, and based on related literature, we identified four relevant factors: Company size, industrial sector, a company's role in the Cloud ecosystem, and the strategic value of IT security. Moreover, we considered the respondent's job function and the division in which he or she works as potential sources for heterogeneity and modeled respective moderator variables.

3.3 Measures

Based on the constructs of the specified structural model a measurement model was developed. Therefore, an initial literature review was conducted in order to identify and classify the major related indicators which semantically describe the structural model's constructs. These indicators were presented to the *Expert Panel* via the aforementioned collaboration system *PBworks*. The experts actively discussed and supplemented the indicator set which was subsequently revised by the authors of this paper and transformed to the study's online questionnaire. Finally, the *Expert Panel* approved[e] the measurement model (including the online questionnaire).

The measurement model includes both formative and reflective elements to account for the methodological problems mentioned in Subsection 3.1. We developed two-construct MIMIC models separating formative and reflective indicators for the major latent variables `Perceived Ease of Use`, `Perceived Usefulness`, `Trust`, and `Adoption`. Within the structural equations model the latent variable is represented by a reflective construct; one or more formative constructs model the composition of the variable [44]. For the reflective (refl.) constructs, existing published measures were applied. Formative (form.) constructs and indicators were based on related work and both specified and validated by the *Expert Panel*. The MIMIC models for `Perceived Usefulness` and `Trust` each consist of one reflective and several formative elements representing the respective benefit and risk dimensions as depicted in Figure 2. In this regard, operational and financial risks were merged to one variable. The remaining two variables were measured linking only one formative element. Table 2 provides an overview of all indicators of the study's primary variables and the variable `Strategic Value of IT Security`. The `Company Size` was determined by means of the company turnover and headcount. The remaining organization-specific factors were each measured by one global indicator with nominal scale.

All indicators were transformed into questionnaire items in German following general construction guidelines [28,46]. As mentioned in the beginning of this section, the supporting expert group validated the wording and soundness of all items as well as the structure of the entire questionnaire from a semantic point of view as suggested by CHURCHILL [47]. SEM requires metrically-scaled data for further analysis [28]. Thus, we applied a systematically constructed seven-point Likert scale, which produces data that can be interpreted metrically for SEM model estimations [28,46].

4 Findings

This section presents the empirical investigation of the research model. In Subsection 4.1, the sample and the process of data collection are described. In Subsection 4.2, implications regarding the market for SECaaS applications are deduced from descriptive data analysis. In Subsection 4.3, the model estimation including quality and hypotheses testing is laid out. Finally, in Subsection 4.4, the results are discussed respecting the research questions of the study.

Table 3 Participants by industrial sector

Class	Percentage	Number
Information technology	44.4%	71
Industry	16.9%	27
Other services	13.1%	21
Public services	10.6%	17
Financial services	8.8%	14
Retail	6.3%	10

Table 5 Participants by role in cloud ecosystem

Class	Percentage	Number
Cloud service	53.8%	86
Consumer (exclusively)		
Cloud service	23.1%	37
Provider (exclusively)		
Cloud service provider	23.1%	37
and consumer		

4.1 Data collection and sample

To carry out the data collection, the measurement model was implemented in an online survey tool and validated by a pre-test with 12 voluntary experts of the *Expert Panel*. In the period from 16 February to 15 April 2011 the survey was accessible via a dedicated Internet address. This address was distributed using the network of the German Federal Association for Information Technology, Telecommunications and New Media. The target population for this study was IT and business professionals who would be involved in their organization's decision-making process regarding the investment in SECaaS. The sample included key informants of provider and consumer organizations of IT solutions in Germany, Austria, and Switzerland and is considered to be representative for potential adopters of SECaaS technologies in the German-speaking area. The survey was preceded by a brief registration. The verified e-mail addresses were stored separately from the survey data in order to guarantee anonymity. The survey (see Additional file 1) began with a landing page including a brief definition of SECaaS, the purpose of the study and its target population, the estimated time expenditure, information about incentives, the privacy policy, and contacts. The questionnaire was divided into six sections.

The survey yielded 202 returns. The data was processed and cleaned as suggested by WEIBER AND MÜHLHAUS [28]. Accordingly, incomplete records were excluded. For the remaining records the squared *Mahalanobis* distances were calculated in order to identify those deviating markedly from the centroid; three outliers were identified and excluded. This left 160 records for further analysis.

The composition of the sample is depicted in Tables 3, 4, 5, 6 and 7 by means of the measured non-metrically scaled organization-specific factors. Of the participating companies, 44.4% originate from the IT sector, which indicates its relatively higher affinity toward SECaaS compared to other industrial sectors (see Table 3). Almost half of the sample (48.1%) consists of large-scale organizations. Medium-sized and smaller organizations each represent about a quarter (see Table 4). Regarding a company's primary role in the Cloud ecosystem, most respondents (53.8%) evaluate their organization to act as exclusive potential consumer of SECaaS. Further 23.1% see their organization in a hybrid role, potentially doing both consuming and providing SECaaS. Only 23.1% do not consider to consume SECaaS at all (see Table 5). Table 6 shows the composition of the sample grouped by the respondents' job function. The majority (37.5%) has an executive position. Also in this regard, most respondents originate from their organization's IT department. Other divisions are under-represented (see Table 7). The variable `Strategic Value of IT Security` was measured by one reflective item on a seven-point *Likert* scale (Mean: 6.244, standard deviation: 1.080). We assume the sample to be compliant with the study's target population and thus representative for the adoption of SECaaS.

4.2 Market implications

The measurement of the study's dependent variable `Adoption` reveals several implications about the market for SECaaS (RQ1). It was measured by two constructs: a reflective element covering the actual use and use intent of SECaaS in regard to the planning horizon, and a formative one containing different security application types. 18.1% of the respondents indicate that their organization is currently using SECaaS. The data further indicates a steadily rising adoption rate. In the long term, over 30% of the surveyed organizations clearly intend to use SECaaS.

Table 4 Participants by company size[f]

Class	Percentage	Number
Small & micro organization	24.4%	39
Medium-sized organization	27.5%	44
Large-scale organization	48.1%	77

Table 6 Participants by job function

Class	Percentage	Number
Manager	37.5%	60
Employee	21.9%	35
IT security officer	13.8%	22
Other	26.9%	43

Table 7 Participants by division

Class	Percentage	Number
Steering committee	10.6%	17
Management and support	17.5%	28
Research & development	5.0%	8
Production	2.5%	4
Information technology	50.6%	81
Sales & marketing	12.5%	20
Other	1.3%	2

Only 16% exclude the possibility of its use entirely. The positive development of the adoption of SECaaS in regard to the organizations' planning horizon is shown in Table 8.

Respondents were asked whether their organization uses or intends to use certain SECaaS application types. *Content Security*, *Endpoint Security*, and *Vulnerability & Threat Management* solutions exhibit especially high adoption rates. Whereas the market is already dominated by the first two application types, the diffusion of Cloud-based *Vulnerability & Threat Management* services is relatively low [14]. This indicates a high level of future adoption, especially for this type of application. Hence, the data indicate a very weak current and future interest in *Compliance & IT Security Management* products. Other types of application are middle-ranking. The overall results and detailed findings specific to industrial sector and company size are summarized in Table 9.

4.3 Model estimation

No adequate global indicators for goodness of model fit exist for PLS-SEM [30,48]. Instead, the measurement model should be estimated first, the structural model afterward [30,49].

4.3.1 Evaluation of the measurement model

The assessment of reflective measurement models includes their reliability and validity [28,30]. An indicator's reliability can be assumed for a minimal factor loading of 0.7 [30,50]. For values between 0.4 and 0.7 indicators should only be eliminated if this increases the construct's *Average Variance Extracted* (AVE) value [30]. Indicators with lower factor loadings indicate deficient reliability and should be removed [30]. According to these requirements, all reflective indicators featured reliability. The reliability of a construct is routinely estimated by means of its *Composite Reliability* (CR) indicating its internal consistency [30]. CR values should be 0.7 or higher [30,49]. This requirement is met for all latent variables. The assessment of the validity of the measurement model includes discriminant validity[g] and convergent validity[h] [30]. Discriminant validity was verified by calculating cross loadings [30]. All indicators have a higher correlation with the appertaining latent variable than with others and thus provide for discriminant validity. Furthermore, for each variable the AVE exceeds the minimal value of 0.5, which indicates the convergent validity of the entire measurement model [30,51]. Table 10 summarizes key metrics of the study's major latent variables including CR and AVE values. For `Attitude` no AVE value was calculated since no formative measures were applied.

Table 8 Development of Adoption[f]

Planning horizon	Percentage with strong positive indication for adoption[a]	Standard deviation	Mean
Currently	18.1%	2.800	2.220
Short-term	24.4%	3.444	2.214
Mid-term	26.3%	3.988	1.939
Long-term	31.3%	4.269	1.856

[a] "strong positive indication" means the selection of 6 or 7 at the 7-point *Likert* scale where 7 represents the strongest intention.

The evaluation of formative indicators aims to support their relevance for the measured construct [30]. This includes the strength and the significance of its influence [28]. The significance can be determined by means of the bootstrap procedure calculating t-values [30]. A formative indicator's influence is assumed to be significant for a t-value = 1.646 (level of significance α = 10%, degrees of freedom df = 1,000). Weights should be 0.1 or higher. Though the results quantitatively indicate the minor relevance of four formative indicators they did not have to be excluded since the *Expert Panel* strongly supported their inclusion from a qualitative point of view [28,30]. Table 11 summarizes weights and significances of the formative indicators for `Perceived Usefulness` grouped by the corresponding benefit dimension. Additionally, the significance of the influence of the respective dimension on the core construct `Perceived Usefulness` (refl.) is shown. In analogy, Table 12 describes the MIMIC measurement model for `Trust`. The measurement model does not contain any redundant formative indicators: the *Variance Inflation Factor* (VIF) indicating multi-colinearity was calculated for all indices. All values (range [1.3; 4.2]) are smaller than the critical value of 5.0; thus, no indicators had to be reconsidered [30,44].

Since the measurement model meets existing requirements entirely, valid estimations of the study's latent variables can be assumed. This is requisite for the subsequent evaluation of the structural model [28,30].

4.3.2 Evaluation of the Structural Model

The evaluation of the structural model includes the degree of determination of the model's latent variables and the

Table 9 Application-specific adoption

Application type	IT	Public services	Financial services	Industry	Other services	Retail	Large-scale organizations	Mid-sized organizations	Small & micro org.	Overall
Content security	●	●	●	●	◕	●	●	◕	●	●
Endpoint security	●	◕	●	◕	◕	◑	●	◕	◕	◕
Vuln. & threat management	●	◕	◑	◕	◔	○	◕	◕	◑	◕
Application security	◕	◕	◔	◕	◑	◑	◑	◑	◕	◑
Identity & access mgmt.	◕	◕	◔	◔	◑	◔	◕	◑	◑	◑
Security info. & event mgmt.	◕	◑	◑	◔	○	◔	◕	◔	◔	◑
Managed devices	◑	◔	◔	◔	◔	◔	◑	◔	◔	◑
Compliance & ITSM	◑	◑	◔	◔	◔	○	◔	◔	◔	◔
				Industrial sector				Org. size		

Very low (0%, ○), low (25%, ◔), medium (50%, ◑), high (75%, ◕), and very high (100%, ●) adoption rate. The range of mean values (range = [1.857; 4.364]) was linearly grouped into five equal classes.

Table 10 Latent variables

Variable	Mean	Standard deviation	R^2	AVE	CR
Adoption	3.444	4.733	.710	.729	.915
Perceived usefulness	4.476	2.983	.663	.849	.944
Perceived ease of use	4.151	2.212	.737	.829	.936
Trust	3.910	3.109	.512	.590	.805
Attitude	3.788	3.053	.587	n.a.	.810

evaluation of the hypothesized relations between them [30]. All independent latent variables meet the required minimal coefficient of determination (R^2) value of 0.3 and are thus sufficiently explained [49] (see Table 10). Due to the study's predictive research goal the R^2 of the dependent variable is of special importance [30]. CHIN suggests a critical value of 0.67 for substantial predictions [49]. This requirement is met for the study's dependent variable `Adoption` (R^2 = 0.71). We additionally proved the model's capacity to predict the dependent variable by means of the *Stone-Geisser* test (cross-validated redundancy $Q^2 = 0.489 > 0$) [30]. Thus, we consider the adoption of SECaaS to be explained comprehensively by this study's proposed model. To test the significances of the model's hypothesized relations, the bootstrap method (df = 1,000) was applied and t-values were calculated [31,52]. In regard to the study's non-directional hypotheses, the influence of one variable on another is considered to be significant when $\alpha = 10\%$ [28,30]. Thus, a hypothesis is supported when the corresponding t-value ≥ 1.646 and the respective null hypothesis is falsified [28]. To get a deeper understanding of the relations we tested three levels of significance: $\alpha = 10\%$ (*, t-value = 1.646); $\alpha = 5\%$ (**, t-value = 1.962); $\alpha = 1\%$ (***, t-value = 2.581). Moreover, corresponding path coefficients were calculated indicating both strength and direction of a variable's influence [28]. According to Lohmoeller path coefficients ≥ 0.1 indicate relevance [53].

All in all 10 of the original 50 hypotheses were supported. Of the hypothesized key determinants only `Attitude` does not have a significant influence on `Adoption`. This might be caused by the consideration of the individual organization-specific factors; however, we did not find any relations between these variables and `Attitude`. The investigation of the MIMIC measurement models of `Perceived Usefulness` and `Trust` revealed that the respective constructs are determined by very few factors. Only quality, and cost and liquidity benefits matter significantly for `Perceived Usefulness`. Ex post we identified the significant influence of `Trust` and `Perceived Ease of Use` on the variable `Perceived Usefulness`. `Trust` is negatively correlated with security risks, social risks, and strategy and compliance risks. Financial and operational risks do not matter. Investigating the organization-specific factors we identified a moderating effect of `Role in Cloud Ecosystem` on the relationship between `Perceived Usefulness` and `Adoption`, and a direct (positive) influence of the `Strategic Value of IT Security` on `Perceived Usefulness`. `Company Size` and `Industrial Sector` do have neither a direct nor indirect influence on the adoption of SECaaS. However, in the course of a more detailed analysis we

Table 11 Formative measurement model for P. usefulness

Formative construct	Indicator weights	Indicator significances (t-Values)	Significance of construct (t-Value)
Cost & liquidity	.270	2.052	2.319**
Benefits	-.631	-4.576	
Quality	.290	2.420	3.632***
Benefits	-.537	-5.138	
Flexibility	.276	1.957	0.754
Benefits	-.613	-5.717	
Focus on	.492	3.044	0.225
Core business	-.601	-3.690	
Improved	.164	1.830	0.700
Resource access	-.635	-5.055	

Table 12 Formative measurement model for trust

Formative construct	Indicator weights	Indicator significances (t-Values)	Significance of construct (t-Value)
Security	.182	1.658	4.450***
Risks	-.453	-3.723	
Social	.278	1.660	1.984***
Risks	-.851	-7.291	
Strategy &	.288	1.706	1.742*
compl. risks	-.524	-4.057	
Financial &	.474	3.375	0.841
op. risks	-.755	-6.918	

found that financial risks matter more for bigger organizations, while social, operational, and strategy and compliance risks are more important to smaller organizations. Figure 3 depicts the reduced model including supported hypotheses. The path coefficients and significances of the hypothesized key drivers are summarized in Table 13.

4.4 Discussion

Below, the findings are discussed in regard to the research questions considering related findings.

4.4.1 RQ1: Is there a market for SECaaS enterprise applications in general and for specific application types in particular?

The market for SECaaS applications is still emerging. The study indicates an already significant and steadily growing acceptance by enterprise consumers. The adoption varies across different security service application types, which supports previous findings about SaaS [23]. The market's focus is on applications for *Content Security*, *Endpoint Security*, and *Vulnerability* & *Threat Management*.

4.4.2 RQ2: Which are the key drivers and inhibitors for the adoption of SECaaS?

Key drivers for the adoption of SECaaS are effort expectancies, perceived usefulness, and trust regarding the adoption of respective applications. These results basically confirm UDOH's findings regarding the adoption of grid and Cloud technologies [26]. Only the influence of the adopter's individual attitude toward the technology [23,26] was not supported for this research context. Hence, the influence of perceived risks and thus the

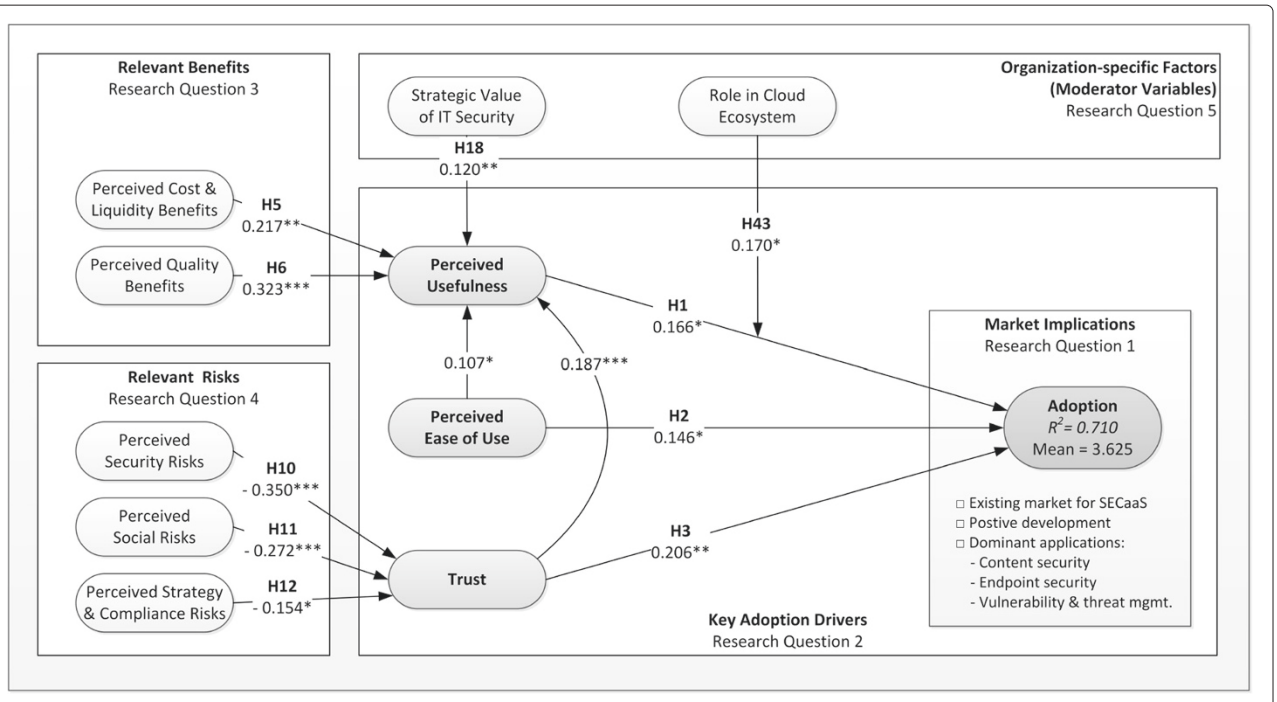

Figure 3 Final model.

Table 13 Estimation of hypothesized key drivers

Hypo-thesis	Relation	Path coefficient	Significance (t-Value)
H1	Perceived usefulness ⇒ adoption	.168	1.912*
H2	Perceived ease of use ⇒ adoption	.146	1.818*
H3	Trust ⇒ adoption	.207	2.333**
H4	Attitude ⇒ adoption	.121	1.453

uncertainty of SECaaS adoption is more significant than the influence of the other drivers, including perceived usefulness. This supports the findings of BENLIAN ET AL. regarding SaaS adoption [23].

4.4.3 RQ3: Which benefits are perceived to be relevant by potential adopters of SECaaS?

The perceived usefulness of SECaaS is forged by quality as well as cost and liquidity benefits. Quality benefits mainly reflect the expected return in terms of an increased level of security and regulative compliance. Cost and liquidity benefits include the reduction of direct security expenditures and recovery costs. Thus, according to the adopter's perception, SECaaS potentially increases return on security investments [54]. Hence, the expected performance of SECaaS systems is positively correlated with effort expectancies and trust, which supports previous empirical findings [22,55,56].

4.4.4 RQ4: Which risks are perceived to be relevant by potential adopters of SECaaS?

Major barriers to SECaaS adoption are perceived security, social, strategy and compliance risks. Perceived social risks are mainly driven by expected internal resistance. In this context, an inherent problem is the possible fear of the direct loss of competencies in the course of outsourcing certain security systems. The significance of social influences regarding SaaS adoption was already identified by BENLIAN ET AL. [23]. To increase trust and thus future adoption the effectiveness of technical and organizational controls securing Cloud-based security services must be conveyed transparently to potential SECaaS consumers. Specific certification programs for service providers might support this, for example.

4.4.5 RQ5: Which organization-specific factors affect the acceptance of SECaaS?

The individual strategic value of IT security for an organization's business directly influences the perceived usefulness of SECaaS. The expected performance is thus higher for organizations with higher demands on IT security from a business point of view. This coherence was already laid out by BENLIAN ET AL. regarding SaaS [23]. Moreover, for the organization's role in the Cloud ecosystem a moderating effect on the relation between the variables `Perceived Usefulness` and `Adoption` was identified. This means that perceived benefits matter less for the actual adoption of SECaaS technologies when the organization itself provides Cloud services for external customers, acting in the role of a *Value Added Reseller* [57]. On the contrary, general organization-specific factors like company size or industrial sector do not have any significant effects on the adoption. This, on the one hand, conflicts with the general rationale that SECaaS is particularly relevant for companies with limited capacities regarding IT security; on the other hand, however, it confirms previous findings regarding the adoption of SaaS [23].

4.4.6 Limitations

The applied methodology (PLS-SEM) is often criticized because calculations tend to be less precise compared to alternative CB-SEM techniques. However, PLS-SEM is more qualified for the application in this study as already laid out in Subsection 3.1. Considering the complexity of this study's research model and the achievable sample size, the application of CB-SEM would not have revealed valid results (compare e.g. [27,28,30]), which supports the authors' research design decision. The sample was selected among organizations with an existing affinity toward IT. Therefore we assume the sample to be representative for potential SECaaS adopters but not for all organizations. The survey explicitly addressed companies in the German-speaking area. Even though it is assumed to provide general insights about the adoption of SECaaS, observations might vary among different markets, for instance due to location-specific data protection regulations. Furthermore, the adoption of SECaaS by private consumers has not been considered and thus remains open for future research.

5 Conclusion

This paper systematically investigates the adoption of SECaaS. An application-specific research model was developed based on existing technology acceptance models. The model was estimated applying the *Partial Least Squares* technique to address the prediction-oriented nature of the study. Based on 160 valid responses from companies in the German-speaking area, we investigated the market potential for SECaaS, key adoption drivers, the relevance of certain risks and benefits, and the influence of organization-specific factors like company size or industrial sector.

The results make valuable contributions for both practice and research. They provide a benchmark for potential adopters of SECaaS. Moreover, the findings support the understanding of the adoption behavior of enterprise

consumers. Service providers can use this understanding to direct research, development and marketing programs by considering the significance of perceived security-related risks, for instance. Therefore, this study contributes to driving the future adoption of SECaaS, addressing existing threats to the security of enterprise information systems. Moreover, the developed research model including its measures was validated and can be applied for related future studies.

Future research should reflect the adoption of Cloud-based security services in other markets, survey specific security application types, investigate most relevant application fields and success drivers.

Endnotes

[a]Session of the "IT security solutions" working group of the German Federal Association for Information Technology, Telecommunications and New Media (BITKOM e.V., see: http://www.bitkom.de last access: 01 August 2012).

[b]http://www.spss.com.hk/statistics/ (last access: 29 September 2012).

[c]16 selected IT and IT security professionals of the German Federal Association for Information Technology, Telecommunications and New Media (BITKOM e.V.).

[d]http://pbworks.com (last access: 01 August 2012).

[e]Therefore, a simple online poll with the options "I do not approve", "I am ok" and "I fully approve" was conducted. Four experts responded "I am ok" and eight fully approved.

[f]According to the European Commission, the number of a company's employees and its turnover (alternatively: balance sheet total) indicate its size. Companies are categorized as follows: "micro", when number of employees $<$ 10 and turnover $\leq$ € 2,000,000; "small", when number of employees $<$ 50 and turnover $\leq$ € 10,000,000; "medium-sized", when number of employees $<$ 250 and turnover $\leq$ € 50,000,000. Larger organizations are labelled as "large-scale". See: http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition (last access: 01 August 2012).

[g]Discriminant validity is provided for when an indicator's loading with the assigned construct is higher than with remaining constructs. An indicator's loading with non-assigned constructs is referred to as cross loading.

[h]Convergent validity expresses the degree to which a latent variable explains the variance of assigned indicators.

Additional file

Additional file 1: Appendix: Online Questionnaire.

Competing interests
The author declare that they have no competing interests.

Received: 6 February 2013 Accepted: 6 February 2013
Published: 4 April 2013

References

1. Hommel W (2007) Architektur- und Werkzeugkonzepte für föderiertes Identitäts-Management. Dr. Hut, München
2. Brock M, Goscinski A (2010) Toward a framework for cloud security. In: Hsu CH, Yang L, Park J, Yeo SS (eds) Algorithms and architectures for parallel processing, Lecture Notes in Computer Science, vol. 6082. Springer, Berlin/Heidelberg, pp 254–263
3. Rittinghouse J, Ransome J (2010) Cloud computing: implementation, management, and security. CRC, Boca Raton
4. Mell P, Grance T (2009) The nist definition of cloud computing. Natl Ins Stand Technol 53 (6): 50. [http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf]
5. Furth B (2010) Cloud computing fundamentals. In: Furth B, Escalante A (eds) Handbook of Cloud Computing. Springer, US, Boston, pp 3–20
6. Höfer C, Karagiannis G (2011) Cloud computing services: taxonomy and comparison. J Internet Serv Appl 2(2): 1–14
7. Gartner Gartner says security delivered as a cloud-based service will more than triple in many segments by 2013 (2008). [www.gartner.com/it/page.jsp?id=722307]
8. Hafner M, Mukhtiar M, Breu R (2009) Seaas - a reference architecture for security services in soa. JUCS 15(15): 2916–2936
9. Peterson G (2009) Service-oriented security indications for use. Comput Sci Eng 7: 91–93
10. Smith DM (2010) Hype cycle for cloud computing 2010. [http://www.gartner.com/DisplayDocument?doc_cd=201557]
11. Staudenrauss P (2011) Untersuchung und Bewertung von Security-as-a-Service-Diensten. In: Helmbrecht U, Kretzschmar M, Eiseler V (eds) Seminar IT-Sicherheit - Sicherheit und Vertrauen in Cloud Computing. Institut füur Technische Informatik, München, pp 49–74
12. Mather T, Kumaraswamy S, Latif S (2009) Cloud security and privacy: an enterprise perspective on risks and compliance. O'Reilly Media Inc, Sebastopol
13. Kark K, Penn J, Whiteley R, Coit L (2010) Market overview: Managed security services. http://www.forrester.com/Market+Overview+Managed+Security+Services/fulltext/-/E-RES56068?objectid=RES56068
14. Senk C, Holzapfel A (2011) Market overview of security as a service systems. In: Pohlmann N, Reimer H, Schneider W (eds) ISSE 2011 Securing Electronic Business Processes
15. Allen J, Gabbard D, May C (2003) Outsourcing Managed Security Services. Carnegie Mellon University Software Engineering Institute. [http://books.google.de/books?id=CFGnNwAACAAJ]
16. Deshpande D (2005) Managed security services: an emerging solution to security In: Proceedings of the 2nd annual conference on Information security curriculum development, InfoSecCD '05. ACM, New York, pp 107–111
17. Keuper F, Wagner B, Wysuwa H (2009) Managed services: IT-Sourcing der nächsten Generation. Gabler. [http://books.google.de/books?id=5J7Qbx2GIYIC]
18. Martens B, Teuteberg F (2011) Decision-making in cloud computing environments: A cost and risk based approach. Inf Syst Front 14(4): 1–23
19. Huber M (2002) IT-security in global corporate networks. Center for Digital Technology and Management, München
20. Karyda M, Mitrou E, Quirchmayr G (2006) A framework for outsourcing is/it security services. Inf Manag Comput Secur 14(5): 402–415
21. Rogers E (2003) Diffusion of Innovations. 5th Edition. Simon & Schuster, New York
22. Venkatesh V, Morris MG, Davis GB, Davis FD (2003) User acceptance of information technology: Toward a unified view. MIS Q 27(3): 425–478
23. Benlian A, Hess T, Buxmann P (2009) Drivers of saas-adoption – an empirical study of different application types. Business Inf Syst Eng 1: 357–369
24. Davis FD, Bagozzi RP, Warshaw PR (1989) User acceptance of computer technology: A comparison of two theoretical models. Manage Sci 35(8): 982–1003
25. Benlian A, Hess T, Buxmann P (2010) Software-as-a-Service: Anbieterstrategien, Kundenbedürfnisse und Wertschöpfungsstrukturen. Gabler, Betriebswirt.-Vlg

26. Udoh E (2010). VDM Verlag Dr. Müller e.K., Saarbrücken
27. Hoyle R (1995) Structural equation modeling: concepts, issues and applications. Sage Publications, New York
28. Weiber R, Mühlhaus D (2010) Strukturgleichungsmodellierung: Eine anwendungsorientierte Einführung in die Kausalanalyse mit Hilfe von AMOS, SmartPLS und SPSS. Springer, Berlin, Heidelberg
29. Edwards JR, Bagozzi RP (2000) On the nature and direction of relationships between constructs and measures. Psychol Methods 5(2): 155–174
30. Hair J, Ringle CM (2011) PLS-SEM: Indeed a silver bullet. J Mark Theory Pract 19(2): 139–151
31. Ringle CM, Wende S, Will A (2005) Smartpls 2.0. http://www.smartpls.de
32. Bliemel F (2005) Handbuch PLS-Pfadmodellierung: Methoden, Anwendung, Praxisbeispiele. Schäffer-Poeschel, Stuttgart, Germany
33. Hamre LJ (2008) Exploring the use of social capital to support technology adoption and implementation. Ph.D. thesis, University of Bath
34. Davis FD (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q 13(3): 319–340
35. Thompson RL, Higgins CA, Howell JM (1991) Personal computing: Toward a conceptual model of utilization. MIS Q 15(1): 125–143
36. Cranor L, Garfinkel S (2005) Security and Usability. O'Reilly Media, Inc, Sebastopol
37. Böhme R (2010) Security metrics and security investment models In: Echizen I, Kunihiro N, Sasaki R(eds) Advances in Information and Computer Security, *Lecture Notes in Computer Science*, vol. 6434. Springer, Berlin / Heidelberg, pp 10–24
38. Schwarze L, Müller, PP (2005) IT-outsourcing - Erfahrungen, status und zukünftige herausforderungen. HMD-Praxis der Wirtschaftsinformatik. http://ephorie.de/pdfs/Schwarze_IT-Outsourcing-Erfahrungen_Status_und_zukuenftige_Herausforderungen.pdf
39. Aubert BA, Patry M, Rivard S (1998) Assessing the risk of IT outsourcing In: Proceedings of the Thirty-First Hawaii International Conference on System Sciences, Volume VI. Organizational Systems and Technology. IEEE Computer Society, Washington, U.S.A., pp 685–693
40. Rouse AC (2009) Is there an "Information technology outsourcing Paradox"? In: Hirschheim R, Heinzl A, Dibbern J (eds) Information systems outsourcing. Springer, Berlin Heidelberg, pp 129–146
41. Duisberg A (2011) Gelöste und ungelöste Rechtsfragen im IT-Outsourcing und Cloud Computing In: Picot A, Götz T, Hertz U (eds) Trust in IT. Springer, Berlin Heidelberg, pp 49–70
42. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34(1): 1–11
43. Fishbein M, Ajzen I (1975) Belief, attitude. Addison-Wesley, Reading
44. Diamantopoulos A, Winklhofer HM (2001) Index construction with formative indicators: An alternative to scale development. J Mark Res 38(2): 269–277
45. Senk C (2010) Securing inter-organizational workflows in highly flexible environments through biometrics In: Proc. of E C I S Pretoria
46. Bortz J, Döring N (2006) Forschungsmethoden und Evaluation für Human- und Sozialwissenschaftler Springer-Lehrbuch. Springer
47. Churchill GA (1979) A paradigm for developing better measures of marketing constructs. J Mark Res 16(1): 64–73
48. Hulland J (1999) Use of partial least squares (pls) in strategic management research: a review of four recent studies. Strateg Manage J 20(2): 195–204
49. Chin WW (1998) The partial least squares approach to structural equation modeling. Modern Methods Business Res 295: 336
50. Johnson MD, Herrmann A, Huber F (2006) The evolution of loyalty intentions. J Mark 70(2): 122–132
51. Fornell C, Bookstein FL (1982) Two structural equation models: Lisrel and pls applied to consumer exit-voice theory. J Mark Res 19(4): 440–452
52. Nevitt J, Hancock GR (2001) Performance of bootstrapping approaches to model test statistics and parameter standard error estimation in structural equation modeling. Struct Equation Model Multidisciplinary J 8(3): 353–377
53. Lohmoeller JB (1989) Latent variable path modeling with partial least squares. Physica, Heidelberg
54. Sonnenreich W, Albanese J, Stout B (2005) Return On Security Investment (ROSI) In: A practical quantitative model Journal of research and practice in information technology. INSTICC Press, Setubal, pp 239–252
55. Lee D, Park J, Ahn J (2001) Proceedings of the International Conference of Information Systems 2001 In: On the explanation of factors affecting E-commerce adoption, pp 109–120
56. Venkatesh V, Bala H (2008) Technology acceptance model 3 and a research agenda on interventions. Decis Sci 2: 273–315. 39
57. Baun C, Kunze M, Nimis J (2010) Cloud computing Web-basierte dynamische IT-services. Springer-Verlag, Berlin and Heidelberg

doi:10.1186/1869-0238-4-11
Cite this article as: Senk: **Adoption of security as a service.** *Journal of Internet Services and Applications* 2013 **4**:11.