Data Privacy in Cloud Computing – An Empirical Study in the Financial Industry

Completed Research Paper

Olga Wenge
Multimedia Communications Lab
Technische Universität Darmstadt
olga.wenge@kom.tu-darmstadt.de

Alexander Müller
Multimedia Communications Lab
Technische Universität Darmstadt
alexander.mueller@kom.tu-darmstadt.de

Ulrich Lampe
Multimedia Communications Lab
Technische Universität Darmstadt
ulrich.lampe@kom.tu-darmstadt.de

Ralf Schaarschmidt
IBM Global Business Services
ralf.schaarschmidt@de.ibm.com

Abstract

Cloud computing is of growing interest due to its potential for delivering scalable and self-managed services. Financial institutions, as “critical users” of cloud computing services, are still slow-going and careful in the usage of clouds, since outsourcing data from a “secure” internal IT infrastructure to an external cloud poses multiple data privacy issues. This paper provides an assessment of the relevance of data privacy requirements, based on interviews with eight representatives of a global international German bank that operates in over 50 countries. Our results indicate that despite technical advancement, administrative countermeasures and legal agreements, certain data privacy issues still form obstacles for the adoption of cloud computing by financial institutions.

Keywords

Cloud computing, financial industry, data security, data privacy, risks, adoption, case study.

Introduction

The emergence of cloud computing and its increasing popularity have brought new benefits for very different industries (Buyya, Yeo, Venugopal, Broberg, and Brandic, 2009). Cloud computing can provide innovative solutions for the companies to reduce cost, improve service performance, and make rapid response to business changes (Heinle and Strebel, 2011). The financial services industry is one of such industries that must react very agilely to changes and thus can be an eligible consumer of cloud computing.

The survey of PricewaterhouseCoopers (2013) concerning challenges in cloud computing market pointed out that areas such as *data privacy*, *compliance requirements*, and *information security* form increasing challenges for companies. This is specifically true for the financial industry as one of the most strictly and complex regulated industrial sectors (Mang, 2010). Due to the current economic situation, the banking industry should reduce IT costs, but without any loss in quality and performance (Farestam, 2009).

For the traditional on-premise model, financial institutions have their own datacenters, hosting and maintenance of infrastructure, whereas cloud computing - like any IT outsourcing - transfers the responsibilities to the service provider (Duisberg, Eckhardt, Grudzien, Hartmann, Hermerschmidt, Kebbedies, Otten, Sieck, Vomhof, Weber, and Weiss, 2011). Given the special requirements in the financial industry, it becomes the major challenge to keep financial data secure, hence preventing incidents such as data leakage, illegal use, or loss of data. Since financial information is directly related to the economic benefits of many groups and individuals, the importance of information security is self-evident (Shi, Xia and Zhan, 2010).

The main goal of data privacy laws and regulations is to protect data and information from unwanted accesses and dispersion (Rittinghouse and Ransome, 2009). Information in the financial industry belongs to the most important assets (or properties) and therefore the protection of this information is one of the most significant objectives for any financial institution (Shue, 2013). Data loss or data leakage can cause reputational damage, penalties, and other legal implications (Rittinghouse and Ransome, 2009).

Based on these observations, we examine the following research question: *Which requirements must be met in cloud computing to ensure data privacy in the financial industry?*

Our contribution is twofold: First, we provide a theoretical analysis of existing data privacy concerns based on financial-sector-specific regulations, laws and legal policies, as well as recommendations with respect to data privacy and map them to the current security solutions. Second, we present the empirical results of a case study, based on interviews with eight security experts employed at an international German bank that conducts global business.

We believe that the results of our work can be of interest to both researchers and practitioners in the area of cloud computing adoption. Furthermore, our work can support cloud providers and cloud consumers in the development of contracts and security solutions for financial institutions.

The remainder of this paper is structured as follows: In the following section, we discuss selected related research results in the area of data privacy and data security in cloud computing. Subsequently, we provide a theoretical analysis of data privacy requirements and existing solutions. Thereafter, we present our methodology and empirical results of our case study. The paper concludes with a brief summary of the main findings and an outlook on our future work.

Related Work

Since the early days of cloud computing, data privacy concerns have been acknowledged as one of the most critical topics by both practitioners and researchers. In the following, we provide a brief overview of this research area, with a specific focus on publications, which are relevant to the work at hand.

Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, Lee, Patterson, Rabkin, Stoica, and Zaharia (2010) place “data confidentiality and auditability” as the third item in the list of “top 10 obstacles” in cloud computing. The authors state that despite the willingness of companies to outsource potentially sensitive services, such as emailing, security concerns are among the “most-cited objections” against cloud computing. Furthermore, the authors outline potential security problems, making the forecast that many issues will be handled through legal agreements, rather than technical solutions.

Ardelt, Dölitzscher, Knahl, and Reich (2011) provide a comprehensive analysis of security problems in the context of cloud computing. The authors distinguish between known IT security problems, which are aggravated through cloud computing, and cloud-specific issues. They analyze the threatened security objectives and propose potential countermeasures for mitigation and full prevention of related security incidents.

Ackermann, Widjaja, Benlian, and Buxmann (2012) provide an in-depth analysis of perceived IT security risks (PITSR) in cloud computing. The authors define perceived risk as “the potential for loss in the pursuit of a desired outcome” and cluster the security issues in order to build a risk taxonomy that involves the risk dimensions confidentiality, integrity, availability, performance, accountability, and maintainability. They further conduct a survey with German companies to validate and evaluate the proposed PITSR measurement instrument. The authors state that perceived IT security risks can “explain the customers’ decisions” in adoption of cloud computing.

In the context of legal aspects of cloud computing in European companies, Sädtler (2013) examines current effective data privacy laws, such as German Federal Data Protection Act (GFDPA) and Data Protection Directive (DPD), and their implications in cloud environments. Sädtler states that “data privacy” is “a very deterrent term” for company managers and is one of “de-motivators for cloud services adoption”. The author further gives an overview of data flow restrictions throughout the European Union and abroad.

Carroll, van der Merwe, and Kotzé (2011) present a qualitative study based on interviews with senior managers of major companies with current or planned implementation of cloud computing. They identify information security as “the biggest cloud computing concern”. Poor third-party management, vendor lock-in, regulations and legislation, and insufficient operations and disaster recovery management are mentioned as additional inhibitors for cloud computing adoption.

Zhou, Zhang, Xie, Qian, and Zhou (2010) provide an empirical survey on security and privacy concerns in cloud computing. The authors interview diverse cloud providers about their perception of security and privacy concerns and weaknesses of existing solutions. Furthermore, the authors analyze effective laws and regulations – such as Electronic Communications Privacy Act (ECPA), Health Insurance Portability and Accountability Act (HIPAA), and Fair Credit Reporting Act (FCRA) – and point out that all of them are not or not fully applicable to cloud computing and should be revised.

Theoretical Analysis of Data Privacy Concerns

In our theoretical analysis, we pursue the aim of reviewing the existing literature and consolidating these findings in a structured manner, thus giving us a basis for the subsequent empirical investigation. As the guideline of our analysis, we used financial-sector-specific regulations and laws to identify requirements with respect to data privacy.

We examined the following data privacy related regulators and regulations, certifications and information security (IS) standards and “best practices”:

- German Federal Data Protection Act (GFDPA) - effective in Germany;
- Data Protection Directive (DPD) - effective in the European Union (EU);
- the Privacy Act - effective in the United States of America (USA);
- Conventions of the Organisation for Economic Co-operation and Development (OECD) - effective in 34 countries;
- Safe Harbor Principles - effective for the USA-EU contracts;
- the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) - effective in the USA;
- the Sarbanes-Oxley Act (SOX) - effective for all enterprises that trade in the USA securities markets;
- the Directive 2006/43/EG or Euro-SOX - effective for all enterprises that trade in the EU securities markets;
- Basel Accords - effective in 20 countries;
- IT Fundamental Right - effective in Germany;
- the Personal Information Protection and Electronic Documents Act (PIPEDA) - effective in Canada;
- the Monetary Authority of Singapore (MAS) - effective in Singapore and in the Asian-Pacific region;
- Bank secrecy acts - effective between banks and customers;
- United States Code (USC) - effective in the USA;
- German Federal Financial Supervisory Authority (GFFSA) - effective in Germany;
- German Banking Act (GBA) - effective in Germany;
- Office of the Comptroller of the Currency (OCC) - effective in the USA;
- Federal Financial Institutions Examination Council (FFIEC) - effective in the USA;
- Statement on Auditing Standards No. 70 (SAS-70) - effective in the USA;
- Binding Corporate Rules (BCRs) - effective in the EU;
- Board of Governors of the Federal Reserve System (BGFRS) - effective in the USA;
- ISO/IEC 27000-series - recommended globally;

- Certified Information Systems Security Professional (CISSP) Principles - recommended globally;
- Certified Information Systems Auditor (CISA) Principles - recommended globally;
- Local territorial laws

Furthermore, we mapped existing technical, physical and administrative solutions to each requirement. The results of our analysis are provided in the Table 1.

Requirement	Corresponding Regulations /Laws	Technical, Physical, and Administrative Solutions

Secure data access	GFDPA; DPD; Privacy Act; OECD; Safe Harbor; Patriot Act; SOX; Euro-SOX; Basel Accords; IT Fundamental Right	Conrad, Misenar and Feldman (2011);
		Stewart, Chapple and Gibson (2012):
		Role-based access; Right-based access;
		Access control lists; Data labeling;
		Need to know principle; Least privilege principle;
		Implementation of ISO/IEC 27000-series controls; Multi-factor authentication;
		Physical access control

Secure personal data transfer	GFDPA; DPD; Privacy Act;
	Safe Harbor; PIPEDA; MAS;
	Bank secrecy; Patriot Act; USC
		Gottschalk (2002); Deutsche Bundesbank (2012); Gentry (2009); Stewart et al. (2012); Conrad et al. (2012); de Meer, Diener, Herkenhöner, Kucera, Niedermeier, Reisser, Guido, Vetter, Waas, and Yasasin (2013); Van Dijk and Juels (2010):
		Anonymization and pseudonymization of data; Virtual Private Network; Data encryption; Securing of transfer channels; Security staff trainings

Prevention of data access through third persons	GFDPA; Privacy Act; Safe Harbor; PIPEDA; MAS; Bank secrecy; Patriot Act	Shue (2013); Conrad et al (2012); Sädtler (2013):
		Access prohibition; Monitoring and logging;
		Physical segregation; Secure data access solutions (see above)

Secure data outsourcing and data processing	GFDPA; DPD; GFFSA; GBA	Deutsche Bundesbank (2013); Sädtler (2013); Weichert (2010); Shue (2013): Legitimate country-specific data transfer monitoring; EU standard contracts with third countries; User consents
Data integrity, confidentiality, availability	GFDPA; DPD; Privacy Act; OECD; Safe Harbor; Patriot Act; SOX; Euro-SOX; Basel Accords; IT Fundamental Right; Bank secrecy	Gill, Bunker and Seltsikas (2011); Conrad et al. (2012); Gentry (2009), Gonzales, Munoz and Mana (2011); de Meer et al. (2013); Van Dijk and Juels (2010): Monitoring and logging; Auditing; Implementation of ISO/IEC 27000-series controls; Data encryption; Public-key infrastructure; Business continuity and disaster recovery measurements

Geographical requirements	GFDPA; DPD; Privacy Act; OECD;
	Local territorial laws
		Sädtler (2013); Sreiberer and Ruppel (2009);
		Weichert (2010); Conrad et al. (2012):

		Contractual obligations; Free data transfer agreements within European Economic Area (EEA); Application of European local territorial laws to branches abroad
Secure cross-border data transactions	GFDPA; DPD; OCC; Local territorial laws	Hasselmeyer and D'Heureuse (2010); Shue (2013); Deutsche Bundesnbank (2013); Conrad et al. (2012); Weichert (2010); Sädtler (2013): Contractual obligations; Monitoring; Auditing
Right to audit	GFFSA; GBA; FFIEC; MAS	Conradt et al. (2012); Deutsche Bundesbank (2013); Shue (2013); Städtler (2013): Cloud provider certifications (e.g., Safe Harbor, SAS-70-Typ-II-Certificate); Binding Corporate Rules; Monitoring and reporting
Transparency of data transfer and data processing	GFFSA; GBA; FFIEC; MAS	Weichert (2010); Deutsche Bundesbank (2013); Shue (2013); Städtler (2013); Klipper (2011): Risk management frameworks; Monitoring and reporting

Compliance	GFFSA; GBA; FFIEC; MAS; BGFRS	Klipper (2011); Weichert (2010); Shue (2013); Deutsche Bundesbank (2013); Conrad et al. (2012); Stewart et al. (2012); Hasselmeyer and D'Heureuse (2010); Mossanen and Amberg (2008):
		Implementation of ISO/IEC 27000-series controls; Payment Card Industry Data Security Standard; Contractual agreements;
		Employee trainings; Information security programs; Monitoring

Security guarantees	GFFSA; GBA; MAS; FFIEC; BGFRS	Klipper (2011); Sädtler (2013); Weichert (2010): Contractual obligations; SLAs
Defined roles and responsibilities	GFFSA; GBA; FFIEC; MAS; BGFRS	Klipper (2011); Weichert (2010); Shue (2013); Deutsche Bundesbank (2013); Conrad et al. (2012); Stewart et al. (2012); Hasselmeyer and D'Heureuse (2010); Mossanen and Amberg (2008): Information security programs; Contractual obligations

Table 1. Data Privacy Requirements and Existing Solutions in Cloud Computing

Empirical Findings from the Financial Industry

Research Methodology

As discussed before, we identified requirements with respect to data privacy issues based on a literature review. We subsequently aligned these requirements with regulations and laws that apply to financial institutions. In addition, we identified the current solutions that can be in place to fulfill the described requirements.

In order to answer, i.e., empirically assess, our research question and examine the practical significance of the previously identified data privacy related issues with respect to the cloud computing adoption in financial institutions, we chose the qualitative research approach, namely a case study. With respect to this instrument, different designs are described in the literature, which exhibit specific advantages and disadvantages (Yin, 2009).

In our work, we conduct a holistic, single-case design. In this context, holistic means that the financial institution as a whole (and not its individual units or departments separately) constitutes the matter of study. As primary data source, we selected the instrument of a personal interview with security experts. On the strength of past experience, this instrument permits a targeted examination of the case study topic and can be highly insightful. However, due to different forms of bias in the responses, the results should also be subject to careful interpretation (Yin, 2009).

As a structural guideline for the interviews, we compiled two questionnaires: a questionnaire with 24 technical questions and a questionnaire with 23 questions concerning legal aspects. Each questionnaire includes three parts. The first, introductory part focuses on the interviewee, his or her organization, and the general understanding of cloud computing. The second part puts the focus on technical or legal aspects of data privacy, and the third part deals with interviewees' expectations on cloud computing.

Using the described questionnaires, we conducted interviews with eight security experts employed by an international German bank that conducts global business. All interviewees work in IT or legal departments of their institute, with a specific focus on information security, and have previously gained professional experience with respect to cloud computing. Due to legal constraints, we refrain from providing additional details about the institute.

Each interview lasted approximately one hour in time. The interviews were digitally recorded and subsequently transcribed into written text. In the following, the interviewees were given the opportunity to review the transcript and make additions or deletions. In accordance with the recommendations by Walsham (1995) and Darke, Shanks and Broadbent (1998), supplemental notes were taken during the interview process by a second researcher to document statements of elevated interest.

The transcripts and notes were analyzed using the method of qualitative content analysis. According to Gläser and Laudel (2010), this method is among the recommended procedures for the analysis of expert interviews. The analysis process involves five steps, including a summary and codification of statements, and ultimately results in deduction of scientific concepts (Cropley, 2005). In contrast to more complex analysis procedures, such as the coding method, the qualitative content analysis requires less initial effort and is thus very well suited for the deduction of preliminary results. Due to space restrictions, the following report of results focuses on a selected set of findings, for which we received the most comprehensive and insightful responses from our interviewees.

Preliminary Results

Given the restricted number of interviews that have been conducted to date, the following results should be considered as preliminary. However, we are confident that our initial results can provide valuable insights with respect to the research question.

To start with, we asked interviewees to their understanding of cloud computing and its relevance to the financial industry. Interviewees confirmed the relevance of all deployment models in their financial institute. All deployment models could be applied to the financial industry, however, "not in equal dimensions". "Private cloud" still stays the dominating deployment model. One interviewee pointed out that the application of other deployment models "currently in its development phase", another interviewee identified deployment models "as already used models, but under a new name - *cloud*".

"Public cloud" was identified as "critical" and "difficult", since the implementation of in-house standards and policies of financial institutes poses a substantial challenge in this specific deployment model. However, the usage of public and hybrid clouds was seen as "possible" solution during "load peaks". "Community cloud" was identified as a possible deployment model "in cooperation with other financial institutions with the same level of implemented security and data privacy standards" for more efficient data exchange. However, one interviewee pointed out that financial institutions "are not willing to share information" due to the "competitive character" of the business.

Interviewees see the advantages of cloud computing in a „homogeneous platform", scalable and quick service provisioning, load peak balancing (equalization), cost reductions, and hardware elimination or replacement. One interviewee pointed out that "non-IT experts can now easier talk about IT" because cloud computing "makes IT comparable". Otherwise, cloud computing is still seen as a new IT paradigm that brings diverse disadvantages due to its "non-transparency and insufficient security controls".

Interviewees specified all business areas, except the ones that involve Personally Identifiable Information (PII), as mostly suitable for cloud usage. Furthermore, data with labels "secret", "confidential" or "strictly-confidential" are seen as ineligible for processing in the cloud. One interviewee pointed out that the fact that "the data is distributed in the cloud and cannot be localized" causes another disadvantage. Insufficient Quality of Service (QoS) guarantees were named as the next "big crux" for the outsourcing of data.

With respect to data integrity, confidentiality and availability, as the main security objectives (Lampe, Wenge, Müller, and Schaarschmidt, 2013), interviewees confirmed that "more attention is paid now" and "the fulfillment of security requirements is on a good way". Furthermore, interviewees stated that if "all three security objectives are achieved", then "all data can be outsourced into the cloud". Such security requirements as "implementation of security controls to protect from data leakage" and "forensic measures to trace activities in the cloud" are seen as compulsory measurements to guarantee data privacy.

Two-factor authentications ("especially for system administrators" and "in conjunction with the usage of public networks"), data encryption and secure data channels were recommended by interviewees as current solutions. Interviewees pointed out that "the same or hardened Authentication, Authorization, and Accountability (AAA) mechanisms must be in place by outsourcing" for employees by the usage of cloud services. Single-Sign-On (SSO) was named as a trustable mechanism between financial institutes and cloud providers, as the storage of passwords by cloud providers is seen as "illegible" and "may not be allowed". Interviewees named the symmetric, asymmetric encryptions, hashing algorithms and fully homomorphic encryption (FHE) as feasible and meaningful encryption approaches for cloud computing.

Concerning secure data transfer in the cloud, interviewees stated that "it is still a big challenge to agree upon the security protection level with a cloud provider, since there are still no standards to be applied" and "different consumers have very different security requirements ". Otherwise, "cloud providers are willing to keep their own flexibility and unique selling points". Interviewees stated that all "data privacy aspects" must be held in contracts. Experts also recommended "constant data encryption by outsourcing".

With respect to the geographical requirements, interviewees expressed a wish to "be always aware of where the data is". Country-specific laws and political situations are seen as critical aspects in outsourcing as well. According to the interviewees, "application of country-specific laws and financial-sector-specific regulations must be well-considered in contracts with cloud providers". MAS, PIPEDA, German Federal Financial Supervisory Authority, German Banking Act, and FFIEC were named as compulsory regulations for financial industry. The EU - and especially Germany, where our case study was conducted – is seen as "currently most secure area for cloud computing", as the "numerous standards and regulations prohibit many actions".

The USA was named as the next possible location for outsourcing, but "only for American citizens without any data privacy concerns". For other users, "additional contracts" must be in place, e.g., Safe Harbor or EU standard contracts in accordance to the local data privacy laws. Regulations and data privacy laws in Argentina, Singapore, Japan, Switzerland, and Turkey were named as "extremely strict", since according to them "no data can be processed abroad".

Concerning the processing of personal data in clouds, interviewees stated that it "must be in accordance with data privacy laws" and banking-sector-specific regulations such as the German Banking Act or the Basel Accords. Compliance to the country-specific data privacy laws were seen by interviewees as the "main hurdle in data transfer". Furthermore, they named encryption, Virtual Private Networks (VPNs), as well as Secure Socket Layer (SSL) and Internet Protocol Security (IPSec) protocols as feasible solutions for securing the data. "User consent" was also seen as "mandatory". MAS was named by interviewees as "the strictest regulator" in the financial industry, since its requirements are "very hard to implement globally".

With respect to the transparency of data processing in clouds, interviewees demanded "full transparency about all actions", "control over all sub-contractors (e.g., helpdesk employees' actions)", and "especially accesses from abroad". Monitoring was named as "the basic and most feasible solution" to bring more transparency into opaque cloud environments. Interviewees pointed also out that only "reasonable" and "risk-driven" monitoring of events makes sense, given that "monitoring of everything is too expensive and time-consuming". "A connecting to in-house monitoring systems" was recommended to "save money and optimize response time for incident management".

The right to audit and compliance with the "in-hose information security policies" are seen by interviewees as mandatory measurements. Experts named the certification of cloud providers as possible solutions – e.g., through SAS70, Safe Harbor, ISO/IEC 27000-series, or Control Objectives for Information and Related Technology (COBIT) –, but described them as "still insufficient" and "too generic due to the absence of cloud standards". "Accurate implementation of in-house security standards" or "equivalent security level" must be guaranteed by cloud providers to provide data privacy in financial institutions as well. According to interviewees, such guarantees must be "agreed in contracts and Service Level Agreements (SLAs)". Interviewees recommended regular staff trainings and background checks by cloud providers' employees as further compliance measures to guarantee secure cloud environments.

Reporting and monitoring were named by interviews as "a very significant part of any information security program". Thereby "data confidentiality, integrity, and availability can be controlled and reported" and financial institutions can still possess control over cloud providers' data accesses. Incident management and business continuity and disaster recovery (BC&DR) management were pointed out as other important measurements to guarantee the availability of data. "Data center mirroring" was named as a mandatory measure to protect data, whereby "minimal distance" between data centers must be considered to guarantee the required response time (RT) and avoid any simultaneous outage of data centers in case of catastrophes (e.g., natural disasters).

The interviewees stated the necessity for "contractual agreements upon all outsourced responsibilities, if such outsourcing is compliant with regulations". In addition, the "accurate definition of all roles and appointments of responsible persons (e.g., Data Privacy Officers)" were pointed out as mandatory measurements. Furthermore, our interviewees demanded the "reporting of any changes in cloud providers' policies" and "exhaustive reporting on occurred incidents".

With respect to the data access through third persons or organizations, interviewees stated country-specific laws as an example of "a legal access". So, according to federal and state laws in the USA, governmental organizations may have an access to personal data, which is prohibited in some other countries, e.g., in Germany or Canada. Interviewees stated "the awareness of such differences in laws" as a necessary requirement to protect data. Furthermore, interviewees demanded "reporting on any third person or third organization access".

In conclusion, interviewees expressed their hope for "a more secure cloud environment" and wished "soon fulfillment of security requirements" from cloud providers' side.

In summary, we found out that many of data privacy requirements relating to cloud computing, which we identified in our theoretical analysis, are also acknowledged by practitioners from the financial industry. In many cases, appropriate monitoring and encryption were named as currently feasible technical countermeasures. In addition, it appears that financial institutions tend to use the instrument of legal agreements and compliance with regulations to mitigate risks and guarantee data privacy for their customers.

Summary and Outlook

Cloud computing as a novel IT paradigm is still in the early development stage. The advantages of cloud computing are obvious, but there are still many doubts about adopting it for practical application in different industries. Financial service industry is one of the industries that can accept the newest technology in the most due to its agility-readiness and willingness to reduce IT costs. However, this industry has the strictest requirements for data privacy, security, and reliability, which caution financial institutions against cloud computing adoption.

In this work, we aimed to analyze whether data privacy requirements and concerns (still) pose an obstacle for the application of cloud computing in the financial industry. For that matter, we identified a set of potential cloud-related data privacy requirements and concerns, based on a survey of current literature, data privacy laws, and industry- and country-specific regulations. Subsequently, we empirically verified our findings through an ongoing case study in the financial industry.

On the basis of eight personal interviews that we have conducted with information security experts from the financial industry, it can be concluded that most of these requirements do, in fact, serve as inhibitors to cloud adoption. It appears that financial institutions focus on both legal and technical solutions to protect data privacy. However, potential for the application of cloud computing is seen across all business areas in the financial industry, if the processing of data sufficiently protected from leakage, loss, and interception, as defined in a multitude of regulatory requirements.

The key challenge for financial institutions, as prospective cloud users, exists in meeting those regulatory requirements and in demanding their fulfillment by external cloud providers; and this is a legal, rather than technical challenge. Many concerns can be resolved through standardization efforts. Therefore, sufficient interoperability among providers (Armbrust et al., 2010) as well as consolidation of diverse data privacy laws (Städtler, 2013) are strongly required.

In addition, our case study indicates that despite progressive development of technical solutions, many of the identified issues will remain challenging in the future. Therefore, it is safe to conclude that financial institutions will continue to provide large parts of their required IT services on-premise in the future, rather than consume them from external cloud providers.

In our future work, we plan to extend our case study and validate the preliminary findings through additional interviews with information security experts from financial institutes and cloud exchanges. Furthermore, through interviews with representatives of cloud service providers, we plan to examine whether the proposed measures in data privacy protection can be applied and enforced in practice.

Acknowledgements

This work has partly been sponsored by E-Finance Lab e.V., Frankfurt am Main, Germany (www.efinancelab.de).

REFERENCES

Ackermann, T., Widjaja, T., Benlian, A., and Buxmann, P. 2012. “Perceived IT Security Risks of Cloud Computing: Conceptualization and Scale Development,” in *Proceedings of the 33rd International Conference on Information Systems*, Orlando, FL, USA, pp. 1-20.

Ardelt, M., Dölitzscher, F., Knahl, M., and Reich, C. 2011. “ Sicherheitsprobleme für IT-Outsourcing durch Cloud Computing, ” *HMD - Praxis der Wirtschaftsinformatik*, (48:281), pp. 62-70.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., and Zaharia, M. 2010. “A View of Cloud Computing,” *Communications of the ACM*, (53: 4), pp. 50-58.

Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., and Brandic, I. 2009. “Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility,” *Future Generation Computer Systems*, (25:6), pp. 599-616.

Carroll, M., van der Merwe, A., and Kotzé, P. 2011. “Secure Cloud Computing: Benefits, Risks and Controls,” in *Proceedings of the South Africa Conference on Information Security*, South Africa, pp. 1-9.

Conrad, E., Misenar, S., and Feldman, J. 2012. *CISSP Study Guide*, Elsevier, Burlington.

Cropley, A.J. 2005. *Qualitative Forschungsmethoden: Eine praxisnahe Einführung*, Klotz, Magdeburg.

Darke, P., Shanks, G., and Broadbent, M. 1998. “Successfully Completing Case Study Research: Combining Rigour, Relevance and Pragmatism,” *Information Systems Journal*, (8:4), pp. 273-289.

de Meer, H., Diener, M., Herkenhöner, R., Kucera, M., Niedermeier, M., Reisser, A., Guido, S., Vetter, M., Waas, T., and Yasasin, E. 2013. “Sicherheitsherausforderungen in hochverteilten Systemen,” *PIK - Praxis der Informationsverarbeitung und Kommunikation*, (36:3), pp. 153–159.

Deutsche Bundesbank. 2013. *BASEL III*, avaliable online: http://www.bundesbank.de/Navigation/DE/Kerngeschaeftsfelder/Bankenaufsicht/Basel3/basel3.html.

Duisberg, A., Eckhardt, J., Grudzien, W., Hartmann, W., Hermerschmidt, S., Kebbedies, J., Otten, G., Sieck, G., Vomhof, M., Weber, M., and Weiss, A. 2011. "Rechtliche Anforderungen an Cloud Computing – Sichere Cloud-Dienste," *IT-Gipfel 2011*, (1:0).

Farestam, S. 2009. "Cloud-Computing - bald Realität für Finanzdienstleister," *Zeitschrift für das gesamte Kreditwesen Technik, (3:4)*, pp. 35–37.

Gentry, C. 2009. *Fully Homomorphic Encryption Scheme*, Stanford University, Diss.

Gill, A.Q., Bunker, D., and Seltsikas, P. 2011. "An Empirical Analysis of Cloud, Mobile, Social and Green Computing: Financial Services IT Strategy and Enterprise Architecture," in *Proceedings of the International Conference on Dependable, Autonomic and Secure Computing*, Sydney, Australia, pp. 697-704.

Gläser, J., and Laudel, G. 2010. *Experteninterviews und qualitative Inhaltsanalyse*, VS Verlag, Wiesbaden.

Gonzales, J., Munoz, A., and Mana, A. 2011. "Multi-layer Monitoring for Cloud Computing," in *Proceedings of the 13th International Symposium on High-Assurance Systems Engineering*, Boca Raton, FL, USA, pp. 291–298.

Gottschalk, S. 2002. *Anonymisierung von Unternehmensdaten: Ein Überblick und beispielhafte Darstellung anhand des Mannheimer Innovationspanels*, ZEW.

Hasselmeyer, P., and D'Heureuse, N. 2010. "Towards holistic multi-tenant monitoring for virtual data Centers," in *Proceedings of the Network Operations and Management Symposium Workshops*, pp. 350–356.

Heinle, C., and Strebel, J. 2010. "IaaS Adoption Determinants in Enterprises," in *Proceedings of the 7nd International Conference on Economics of Grids, Clouds, Systems, and Service*, Ischia, Italy, pp. 93-104.

Klipper, S. 2011. *Information Security Risk Management: Risikomanagement mit ISO/IEC 27001, 27005 und 31010*. Vieweg+Teubner.

Lampe, U., Wenge, O., Müller, A., and Schaarschmidt, R. 2013. "On the Relevance of Security Risks for Cloud Adoption in the Financial Industry," in *Proceedings of the 19th Americas Conference on Information Systems*, Chicago, IL, USA, pp. 1–8.

Mang, F. 2010. "Herausforderungen für die IT im Bankensektor," *Zeitschrift für das gesamte Kreditwesen*, pp. 10–12.

Mossanen, K., and Amberg, M. 2008. "IT-Outsourcing & Compliance," *HMD – Praxis der Wirtschaftsinformatik* (45:263), pp. 58–68.

PricewaterhouseCoopers 2013. *Cloud Computing Evolution in the Cloud*, available online: http://www.pwc.de/de_DE/de/prozessoptimierung/assets/cloud_computing_2013.pdf.

Rittinghouse, J., and Ransome, J. 2009. *Cloud computing: implementation, management, and security*, CRC press.

Sädtler, S. 2013. "Aktuelle Rechtsfragen des Datenschutzes und der Datensicherheit im Cloud Computing," *PIK - Praxis der Informationsverarbeitung und Kommunikation*, (36:3), pp. 165–173.

Shue, L. 2013. *Sarbanes-Oxley and IT Outsourcing*, available online: http://www.isaca.org/Journal/Past-Issues/2004/Volume-5/Documents/jpdf045-Sarbanes-OxleSandITOutsou.pdf.

Shi, A., Xia, Y., and Zhan, H. 2010. "Applying Cloud Computing in Financial Service Industry," in *Proceedings of the International Conference on Intelligent Control and Information Processing*, Dalian, China, pp. 579-583.

Stewart, J., Chapple, M., and Gibson, D. 2012. *Certified Information Systems Security Professional, Study Guide*, John Wiley & Sons.

Streitberger, W., and Ruppel A. 2009. *Cloud Computing Sicherheit – Schutzziele. Taxonomie.* Marktübersicht, Fraunhofer AISEC.

Van Dijk, M., and Juels, R. 2010. "On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing," *IACR Cryptology ePrint Archive*, pp. 305–311.

Walsham, G. 1995. "Interpretive Case Studies in IS Research: Nature and Method," *European Journal of* Information Systems, (95:4), pp. 74–81.

Yin, R.K. 2009. Case Study Research – Design and Methods, Sage Publications, Thousand Oaks.

Zhou, M., Zhang, R., Xie, W., Qian, W., and Zhou, A. 2010. "Security and Privacy in Cloud Computing: A Survey," in *Proceedings of the 6th International Conference on Semantics Knowledge and Grid*, Beijing, China, pp. 105–112.