Cloud Computing in the Financial Industry – A Road Paved with Security Pitfalls? [PRE-PRINT]

Ulrich Lampe
Multimedia Communications Lab (KOM) – Technische Universität Darmstadt, Germany
ulrich.lampe@KOM.tu-darmstadt.de

Olga Wenge
Multimedia Communications Lab (KOM) – Technische Universität Darmstadt, Germany
olga.wenge@KOM.tu-darmstadt.de

Alexander Müller
Multimedia Communications Lab (KOM) – Technische Universität Darmstadt, Germany
alexander.mueller@KOM.tu-darmstadt.de

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

ABSTRACT

In the financial industry, Information Technology (IT) is an essential production factor, but also a major expense post. Because cloud computing promises to deliver IT services more flexibly and cost-efficiently, it potentially constitutes a "perfect match" for the financial sector. However, given the high degree of regulation, concerns regarding security and compliance requirements arise. In this work, we provide a detailed theoretical analysis of potential security problems in the context of cloud computing. This analysis is complemented by the initial results of an ongoing case study concerning the practical relevance of these problems in the financial industry. The analysis confirms that security issues pose notable obstacles for the adoption of cloud computing in practice, but also points to appropriate countermeasures.

Keywords

Cloud computing, financial industry, banking industry, security, compliance, analysis, case study.

INTRODUCTION

In the financial industry, the collection, processing, and dissemination of large amounts of information constitute the basis for many, if not all, business processes (Berger, 2003). Accordingly, financial institutions are among the most intensive users of Information Technology (IT)[1] across various service industries (Triplett and Bosworth, 2006).

Following some controversy about the "productivity paradox" of IT in the late 1980s and early 1990s, it has been empirically validated since that investments in IT may – specifically in the banking industry – result in substantial returns, cost savings,

[1] In accordance with Brynjolfsson and Hitt (2000), we interpret IT as „computers as well as related digital communication technology".

and increases in market share (Prasad and Harker, 1997; Brynjolfsson and Hitt, 2000; Ho and Mallick, 2009). Besides its role as a "backbone" of most finance-related business processes, IT can also serve as an "enabler" for novel products. Prominent examples include online banking, electronic payment methods, or automatic teller machines (Berger, 2003; Lamberti and Büger, 2009).

Due to the constant decline in the absolute cost of IT equipment, many financial institutions have historically replaced other production factors with IT. This has led to a further increase in the relative importance of IT, compared to other production factors such as human labor (Casolaro and Gobbi, 2005). As a result, IT constitutes a major expense post for most financial institutions today. For instance, in 2001, Italian banks spent 8.0% of their gross income and 14.5% of their operating costs on IT (Casolaro and Gobbi, 2005). More recent estimates confirm this magnitude order and attribute between 15% and 20% of banks' overall administrative expenses to IT expenses (Moormann and Schmidt, 2007).

Lately, cloud computing has arrived as a novel IT paradigm that promises to "revolutionize" the way IT services are provisioned and consumed (Leymann, 2009). The essential idea of cloud computing is to deliver IT services – such as compute infrastructure or storage – in a utility-like manner (Buyya, Yeo, Venugopal, Broberg and Brandic, 2009), thus making these services ultimately more flexible and cost-efficient (Leymann, 2009). Given the role of IT in the financial services sector, as an essential production factor, but also a major expense post, cloud computing may seem as a "perfect match" for this industry.

However, there appears to be one major obstacle: security. In fact, a recent survey by the IT Governance Institute (2011) confirmed that general security concerns and data privacy concerns constitute the most severe reasons for *not* using cloud computing. In accordance, the aspect of "data confidentiality and auditability" is also seen among the top 10 obstacles to the growth and application of cloud computing in one of the seminal papers on cloud computing (Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, Lee, Patterson, Rabkin, Stoica and Zaharia, 2010). It is reasonable to conclude that these concerns are especially pronounced in the financial industry, which is among the most regulated sectors (White, 1997), and thus subject to rigid data privacy and security requirements. Thus, the initial notion of a perfect match between cloud computing and the financial industry appears doubtful.

Based on these observations, we examine the following research question in the work at hand: "*Do security concerns pose an obstacle for the adoption of cloud computing in the financial industry and, if yes, which concerns specifically"*? Our contribution is twofold: First, we provide a theoretical analysis of potential security problems in conjunction with the application of cloud computing. Second, we present the initial empirical results of an ongoing case study, which involved two interviews with representatives of an internationally operating German bank.

The remainder of this work is structured as follows: In the following section, we provide an introduction into the fundamental concepts of cloud computing. In the subsequent section, we analyze potential security and compliance issues in conjunction with the use of cloud computing in the financial industry. Thereafter, we present the methodology and results of our ongoing empirical research. The paper concludes with a brief summary and outlook.

FUNDAMENTALS OF CLOUD COMPUTING

While the term cloud computing is currently very popular in research and practice today, no commonly accepted definition exists so far (Vaquero, Rodero-Merino, Caceres and Lindner, 2009). Recently, however, the definition by the *National*

Institute of Standards and Technology (NIST) has emerged as a de-facto standard; it states that "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources" (Mell and Grance, 2011). Such resources may include virtually any type of computing capabilities, including "networks, servers, storage, applications, and services" (Mell and Grance, 2011).

In addition, the definition names five essential characteristics: First, the ability for consumers to commission and decommission capacities in an autonomous manner (on-demand self-service); second, the provision of capacities to heterogeneous end-user devices via the Internet (broad network access); third, the pooling and subsequent provision of resources according to a multi-tenant model, often based on virtualization techniques (resource pooling); fourth, the ability to rapidly add or remove capacities (rapid elasticity); fifth, a metered service provision, often based on a pay-per-use model (measured service).

Mell and Grance (2011) have further defined a basic taxonomy of cloud systems, which distinguishes four common deployment and three service models. An overview is depicted in Figure 1.

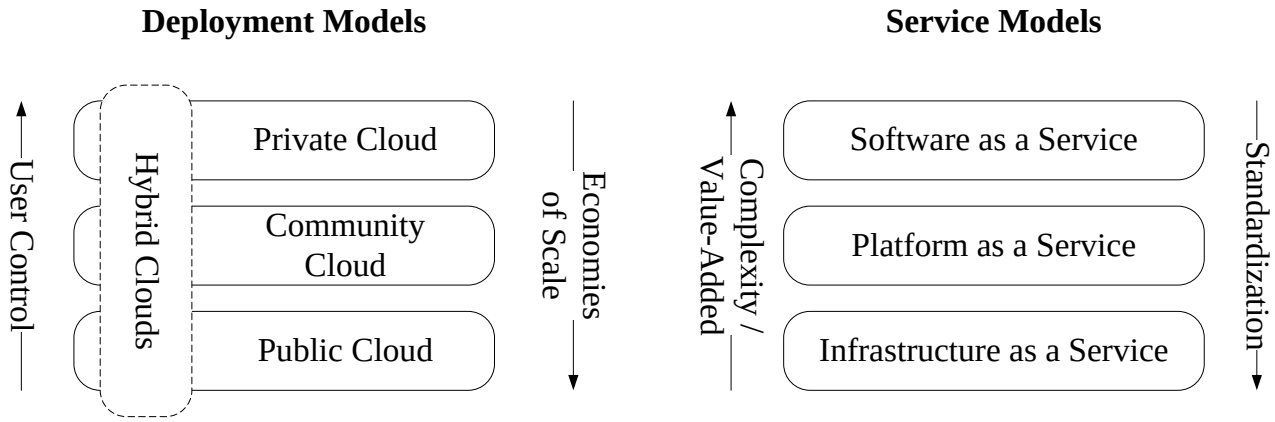

Figure 1: Common cloud deployment and service models

The *deployment models* essentially refer to the relationship between service provider and service consumer (also referred to as service user). In the case of a *private cloud*, a service is offered to one exclusive consumer, either by a provider from the same organization or by an external party. A *community cloud*, in contrast, is restricted to a pre-defined set of consumers, rather than an individual consumer. Lastly, a *public cloud* is operated by a specialized vendor; it is open to the general public or a large group of consumers. The term *hybrid cloud* can refer to any combination of aforementioned deployment models. In general, economies of scale increase moving from a private to a public cloud, whereas the control of the user over the overall cloud system decreases.

The service models refer to the level of complexity that a cloud service provides. *Infrastructure as a Service* (IaaS) includes the provision of rather low-level IT capabilities, such as storage or compute power. *Platform as a Service* (PaaS) refers to somewhat more sophisticated offers, such as programming and execution environments. Lastly, *Software as a Service* (SaaS) includes complex applications, which are often operated on the basis of IaaS or PaaS services (Lenk, Klems, Nimis, Tai and Sandholm, 2009). In general, the complexity of the services increases moving from IaaS to SaaS, whereas the degree of (technical) standardization appears to decrease.

For further details on the fundamentals of cloud computing, we refer the interested reader to Armbrust et al. (2010), Buyya et al. (2009), or Leymann et al. (2009). A more detailed taxonomy, including various examples of actual cloud service offers, has been provided by Lenk et al. (2009).

THEORETICAL ANLAYSIS OF CLOUD COMPUTING SECURITY ISSUES

Recently, a growing number of researchers have been concerned with the issue of security in cloud computing. In our theoretical analysis, we pursued 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 the ten security domains of the well-known *Certified Information Systems Security Professional* (CISSP) certificate[2]. These domains cover diverse aspects of security, ranging from physical security of computing facilities, business continuity planning for disaster scenarios, to the application of cryptography techniques (Harris, 2010; Conrad, Misenar and Feldman, 2010). Most of these domains can be found in identical or comparable form in other IT security guides, e.g., by the Cloud Security Alliance (2011) or the Information Systems Audit and Control Association (2011). Thus, while not specifically tailored to cloud computing, but rather IT in general, the CISSP domains provide a comprehensive scheme for the classification of security issues. Accordingly, we mapped each security problem or risk that we found in the literature onto one of the ten CISSP domains.

In addition, we identified specific security objectives that may be threatened by each problem or risk. In this context, we focused on the three "classic" security objectives of confidentiality, integrity, and availability, which have been well-known for many years as part of the so-called "CIA triad" (Johnson, 2010; Conrad et al., 2010). Confidentiality describes that information may only be read by authorized parties; in this context, authorization refers to the fact that these parties possess appropriate access rights (Johnson, 2010). A tangible example from the financial industry account or credit card information, which constitutes sensitive personally identifiable information and should only be disclosed to the appropriate stakeholders, e.g., for clearing purposes, cf. (Conrad et al., 2010). Integrity is defined very similarly, but refers to writing (i.e., modifying or deleting) information (Johnson, 2010; Conrad et al., 2010). Again, with respect to the financial industry, a tangible example would consist in the modification of an account balance. Lastly, availability means that information or a system is accessible in a timely and reliable way whenever needed (Johnson, 2010).

The results of theoretical analysis are provided in summarized form in Table 1. The table lists a total of 23 potential security problems or risks in the context of cloud computing. As previously explained, the problems are organized along the ten CISSP security domains. In addition, the threatened security objectives and corresponding literature sources are stated.

We acknowledge that not all of the provided problems are necessarily exclusive to cloud computing or apply to all deployment and service models. However, we do believe that all of the given items bear relevance with respect to the application of this novel IT paradigm in the financial industry.

[2] The CISSP certificate is issued by *The International Information Systems Security Certification Consortium, Inc.* (https://www.isc2.org/).

Table 1: Potential security problems and risks in cloud computing

No.	CISSP Domain	Problem or Risk	Threatened Security Objective[3]	Source(s)
1	1 – Information Security Governance and Risk Management	Insufficient security monitoring policies	C, I, A	Hubbard and Sutton, 2010; Ardelt et al., 2011
2		Lack of interoperability between cloud service providers	C, I, A	Armbrust et al., 2010; Hubbard and Sutton, 2010; Ardelt et al., 2011
3		Lack of data transparency concerning data deletion handling	C, I	Armbrust et al., 2010; Hubbard and Sutton, 2010; Ardelt et al., 2011;
4		Partial failure of a cloud service	I, A	Streitberger and Ruppel, 2009
5	2 – Access Control	Abuse of administrative privileges or rights	C, I, A	Hubbard and Sutton, 2010; Ardelt et al., 2011
6		Abuse or theft of user accounts	C, I, A	Armbrust et al., 2010; Conrad et al., 2010, Hubbard and Sutton, 2010
7	3 – Cryptography	Decryption and temporary storage of content within the cloud	C	Gross et al., 2011
8		Concurrent access to encrypted data / lack of isolation in multi-tenancy	C, I, A	Hubbard and Sutton, 2010; Ardelt et al., 2011; Karlinger et al., 2011
9	4 – Physical (Environmental) Security	Failure of hardware devices	A	Conrad et al., 2010
10		Risk of an electricity blackout	A	Conrad et al., 2010
11	5 – Security Architecture and Design	(Distributed) Denial of Service attacks	A	Jensen et al., 2009; Armbrust et al., 2010; Conrad et al., 2010; Gross et al., 2011
12		Cloud-based man-in-the-middle attack (Janus attack)	C, I, A	Gross et al., 2011
13		Virtual machine escape attack	C, I, A	Grobauer et al., 2011
14		Root access to IaaS instances	C, I, A	Ardelt et al., 2011
15		Vulnerability of user-facing Web interfaces to network attacks	C, I, A	Jensen et al., 2009; Hubbard and Sutton, 2010; Ardelt et al., 2011; Gross et al., 2011,
16		Use of an insecure Application Programming Interface (API)	C, I, A	Jensen et al., 2009; Hubbard and Sutton, 2010; Ardelt et al., 2011
17	6 – Business Continuity Planning and Disaster Recovery Planning	Failure of the communication link or data center	A	Armbrust et al., 2010; Conrad et al., 2010
18	7 – Telecommunications and Network Security	Depletion of available communication capacity	A	Conrad et al., 2010
19		Depletion of available resource pool or monetary budgets	A	Jensen et al., 2009; Ardelt et al., 2011
20	8 – Application Development Security	Lack of transparency concerning applied security mechanisms	C, I, A	Hubbard and Sutton, 2010; Ardelt et al., 2011
21	9 – Operations Security	Lack of transparency concerning rules governing security events	C, I, A	Hubbard and Sutton, 2010; Ardelt et al., 2011
22		Abuse of cloud resources	A	Hubbard and Sutton, 2010; Ardelt et al., 2011
23	10 – Legal, Regulations, Investigations, and Compliance	Migration of data between different data center locations	C	Streitberger and Ruppel, 2009

[3] Abbreviations: Confidentiality (C), Integrity (I), Availability (A)

EMPIRICAL INVESTIGATION IN THE FINANCIAL INDUSTRY

Methodology

In order to empirically assess our research question and examine the practical significance of the previously identified, cloud computing-related security issues, we chose the qualitative research approach of 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 pursue a holistic, multi-case design. In this context, holistic means that financial institutions as a whole – and not their individual units or departments – constitute the matter of examination. We chose a multi-case design due to the potentially higher robustness and explanatory power of such design (Yin, 2009). As primary data source, we selected the instrument of personal interviews with domain experts. As major strengths, 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 the basis for the interviews, we compiled a questionnaire consisting of roughly 40 individual questions. Using this questionnaire, we conducted interviews with two representatives of a German bank[4]. Both interviewees work in the IT department of their institute, with a specific focus on IT security, and have previously gained professional experience with respect to cloud computing. In the following, we will refer to the interviewees as *A* and *B*.

Each interview lasted approximately one hour in time. Both 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 recommend 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.

Preliminary Results

Given the restricted number of interviews that have been conducted to date, the following results should be considered preliminary. In addition, because both interviewees are associated with a bank, the discussion of results focuses on the banking industry, rather than the financial services sector in general. However, we are confident that our initial results can provide valuable insights with respect to the research question.

To begin with, the interviews confirmed the notion that the term cloud computing is interpreted very widely. Specifically, interviewee B stated that “[cloud computing is] a dazzling term, which is used for a multitude of things and not clearly

[4] For reasons of anonymity, we refrain from providing additional details about the institute.

defined." In general, the interviewees agreed, however, that cloud computing involves the provision of services from a shared environment via a (public) network. These services are standardized and ready-to-use.

All three service models in cloud computing are of relevance to the banking industry. However, according to the interviewees, cloud computing will not be the dominant delivery model in any business area, because some processes cannot be outsourced to third parties. Business areas such as investment banking, which are subject to constant change, are specifically suited for the application of cloud computing.

Among the delivery models, private cloud computing has the highest relevance. A private cloud can serve as central service, which is used by the financial institute itself or its outsourced partners. According to the interviewed bank representatives, the public cloud computing delivery model has limited practical significance in the banking industry. Yet, interviewee B pointed to the "successive entry of cloud services, which are offered in the consumer area [into the business world]". He added, however, that the proof is yet to be made that "cloud services can establish themselves [in the financial industry]"

According to both interviewees, IT in the banking sector is subject to a broad range of risks. These risks relate to people, processes, systems, and external factors. Damages may not only concern virtual goods, but also physical goods, such as data centers, facilities, or employees. Interviewee A also pointed to non-financial damages, for instance "risks in terms of reputation". Interviewee B sees the inability to judge the reliability of cloud services as a major problem, given that processing failures may lead to substantial risks for the institute.

With respect to the first CISSP domain, "information security governance", both interviewees saw the application of appropriate monitoring as an essential prerequisite for the use of cloud services. Thus, according to interviewee B, a cloud provider will have to comply with "extensive manuals and policies" and certify its adherence to those rules. As a specific technical mechanism, interviewee A named the use of trusted platform modules, which guarantee that "only warranted operations can be conducted on specific data". In addition, the encryption of critical data is seen as an appropriate measure. Interviewee B did not see the risk of a vendor lock-in with standardized services in the banking industry. Still, banks should be very aware about the dependence on specific vendors. In that context, interviewee B stressed that "banks would not be willing to cooperate with a monopolistic provider".

Concerning the second CISSP domain, "Access Control", interviewee B saw the risk of an abuse of administrative privileges as valid scenario, with enormous potential for attacks. Thus, administrative personnel should "underlie a detailed monitoring". Both interviewees pointed out that critical data, including authentication credentials, should always be transferred via secured channels. With respect to the theft of user accounts, "two-factor authentication" was named as a technical countermeasure.

In the context of the third CISSP domain, "Cryptography", both bank representatives stressed the significance of appropriate monitoring solutions to address potential security issues. As a technical measure, interviewee A further pointed to the use of client-based encryption mechanisms, which ensure that data "is [exclusively] written back to the cloud in encrypted form" (i.e., end-to-end encryption is enforced). Both interviewees further stressed that the distinction between data-at-rest and data-in-transit is important for the choice of appropriate security mechanisms, such as channel encryption.

With respect to the fourth CISSP domain, "Physical Security", the use of appropriate monitoring solutions and enforcement of policies at the cloud provider is seen as important aspect again. Both bank representatives agreed that potential damages do

not only concern virtual, but also physical goods, such as data centers or facilities. In this respect, interviewee A believes that "cyber war and cyber terrorism will play a certain role [in the future]".

Concerning the fifth CISSP domain, "Security Architecture and Design", interviewee B identified the comprehensive training of employees as an important measure to raise the awareness of security problems. This does not only concern "the employees [of the institute itself], but everyone you has access to a company's systems, because today, multiple [external] service providers are employed". In this context, interviewee A specifically pointed to the risk through cloud-based man-in-the-middle attacks, saying that a lack of awareness at both the user and provider side would create "completely new opportunities", specifically with respect to eavesdropping. Once again, trusted platform modules are perceived as a viable technical countermeasure to address many security problems.

With respect to the sixth CISSP domain, "Business Continuity Planning (BCP)", the failure of communication channels, namely access to the Internet, was acknowledged as a relevant risk. Interviewee A named legal agreements with the network providers as appropriate countermeasure, saying that "depending on the risk of the processed data […] there has to exist a disaster recovery scenario […] in the case of a cloud setting; you have to be able to substitute [network capabilities]".

In the context of the seventh CISSP domain, "Telecommunications and Network Security", the interviewed bank representatives stressed the importance of monitoring to detect attacks that aim at an exploitation of network or computing capacities. Interviewee A further stated that redundant resources should be made available, depending on the criticality of systems or data.

With respect to the eighth and ninth CISSP domains, "Application Development Security"[5] and "Operations Security", both interviewees referred to the same mechanisms that were previously discussed with respect to the first domain. This includes the use of appropriate monitoring mechanisms and the enforcement of policies by the bank as service user.

Lastly, concerning the tenth CISSP domain, "Legal, Regulations, Investigations, and Compliance", interviewee B acknowledged that the inability to localize data in clouds may constitute an important obstacle for their adoption, given that this situation may result in judicial or regulatory problems. Once again, monitoring is seen as a potentially appropriate countermeasure. The physical location of data most notably plays a major role due to different jurisdictions. As a specific example, German banks may not transfer data to the United States despite of the Safe Harbor agreement, because – according to interviewee B – "US authorities may access this data if investigations are ordered".

In summary, we found that many of the security issues with cloud computing that we identified in our theoretical analysis are also acknowledged by practitioners from the industrial practice. In many cases, appropriate monitoring or trusted platform solutions are named as appropriate technical countermeasures. In addition, it appears that banks tend to use the instrument of legal agreements and compliance rules to mitigate risks and shift the financial responsibility for security issues to the cloud providers.

[5] As of January 1st, 2012, this domain has been renamed to "Software Development Security".

SUMMARY AND OUTLOOK

In the financial industry, IT is one of the substantial production factors, and its relative importance has steadily increased in recent decades. However, IT also poses a major expense post. Cloud computing is a novel architectural paradigm that promises to revolutionize the way IT services are provisioned and consumed. Due to its potential for cost-savings and its flexibility, cloud computing may appear as a perfect match to the financial industry. However, security concerns have recently been named as a potential sticking point for the adoption of cloud computing, specifically in the financial industry which is subject to a multitude of regulatory requirements.

In this work, we aimed to analyze whether security concerns pose an obstacle for the application of cloud computing in the financial industry. For that matter, we identified a set of potential cloud-related security risks, based on a survey of current literature. Subsequently, we empirically verified our findings through an ongoing case study in the financial industry.

According to the interviews with two representatives of a German bank, security concerns do in fact constitute an obstacle for the adoption of cloud computing. This is specifically true with respect to the public cloud computing deployment model. Accordingly, this model is only applied to a very limited extent at present. However, potential for the application of cloud computing is seen across all business areas in the financial industry.

On the basis of the case study analysis, it appears that banks focus on both legal and technical measures to address potential security problems. The former include legal agreements with cloud providers and the enforcement of security-related manuals and policies; the latter include the use of encryption and trusted platform modules.

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

REFRENCES

1. Ardelt, M., Dölitzscher, F., Knahl, M. and Reich, C. (2011) Sicherheitsprobleme für IT-Outsourcing durch Cloud Computing, *HMD - Praxis der Wirtschaftsinformatik*, 48, 281, *62-70.*
2. 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, 50-58.
3. Berger, A.N. (2003) The Economic Effects of Technological Progress: Evidence from the Banking Industry, *Journal of Money, Credit, and Banking*, 35, 2, 141-176.
4. Brynjolfsson, E. and Hitt, L.M. (2000) Beyond Computation: Information Technology, Organizational Transformation and Business Performance, *The Journal of Economic Perspectives*, 14, 4, 23-48.
5. 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, 599-616.
6. Casolaro, L. and Gobbi, G. (2005) Information Technology and Productivity Changes in the Banking Industry, *Economic Notes*, 36, 1, 43-76.

7. Cloud Security Alliance (2011) Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. [Online] https://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
8. Conrad, E., Misenar, S. and Feldman, J. (2010) CISSP Study Guide, Elsevier, Burlington.
9. Cropley, A.J. (2005) Qualitative Forschungsmethoden: Eine praxisnahe Einführung (2nd ed.), Klotz, Magdeburg.
10. Darke, P., Shanks, G. and Broadbent, M. (1998) Successfully Completing Case Study Research: Combining Rigour, Relevance and Pragmatism, *Information Systems Journal*, 8, 4, 273-289.
11. Gläser, J. and Laudel, G. (2010) Experteninterviews und Qualitative Inhaltsanalyse (4th ed.), VS Verlag, Wiesbaden.
12. Grobauer, T., Walloschek, T. and Stöcker, E. (2010) Understanding Cloud Computing Vulnerabilities, *IEEE Security & Privacy*, 9, 2, 50-57.
13. Groß, S., Gruschka, N., Jensen, M., Lischka, M., Miede, A., Mosch, M., Schulte, S. and Siebenhaar, M. (2011) Sicherheitsprobleme im Cloud Computing, *Praxis der Informationsverarbeitung und Kommunikation*, 34, 3, 126-134.
14. Harris, S. (2010) CISSP Certification All-in-One Exam Guide (5th ed.), McGraw-Hill, New York.
15. Ho, S.J. and Mallick, S.K. (2009) The Impact of Information Technology on the Banking Industry, *Journal of the Operational Research Society*, 61, 2, 211-221.
16. Hubbard, D. and Sutton, M. (2010) Top Threats to Cloud Computing V1.0. [Online] https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
17. Information Systems Audit and Control Association (2011) IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud, Information Systems Audit and Control Association, Rolling Meadows.
18. IT Governance Institute (2011) Global Status Report on the Governance of Enterprise IT (GEIT) – 2011, IT Governance Institute, Rolling Meadows.
19. Jensen, M., Schwenk, J., Görtz, H. and Gruschka, N. (2009) On Technical Security Issues in Cloud Computing, In: Liang-Jie Zhang, (Ed.) *Proceedings of the 2nd IEEE International Conference on Cloud Computing*, September 21-25, Bangalore, India, IEEE, 109-116.
20. Johnson, B.C. (2010) Information Security Basics, *ISSA Journal*, 8, 7, 28-32.
21. Karlinger, M., Ettmayer, K. and Schrefl, M. (2011) Verschlüsselung bei ausgelagerter Datenhaltung, *HMD - Praxis der Wirtschaftsinformatik, 48*, 281, 35-43.
22. Lamberti, H.J. and Büger, M. (2009) Lessons Learned: 50 Years of Information Technology in the Banking Industry - The Example of Deutsche Bank AG, *Business & Information Systems Engineering*, 1, 1, 26-36.
23. Lenk, A., Klems, M., Nimis, J., Tai, S. and Sandholm, T. (2009) What's Inside the Cloud? An Architectural Map of the Cloud Landscape, In: Kamal Bhattacharya, Martin Bichler, Stefan Tai (Eds.), *Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing*, May 23, Vancouver, Canada, IEEE, 23-31.
24. Leymann, F. (2009) Cloud Computing: The Next Revolution in IT, In: Dieter Fritsch (Ed.), *Proceedings of the Photogrammetric Week '09*, September 7-11, Stuttgart, Germany, Wichmann Verlag, 3-12.
25. Mell, P. and Grance, T. (2011) The NIST Definition of Cloud Computing (Draft). [Online] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

26. Moormann, J. and Schmidt, G. (2007) IT in der Finanzbranche, Springer-Verlag, Berlin / Heidelberg.
27. Prasad, B. and Harker, P.T. (1997) Examining the Contribution of Information Technology Toward Productivity and Profitability in US Retail Banking, *The Wharton Financial Institutions Center Working Papers*, 97, 9.
28. Streitberger, W. and Ruppel A. (2009) Cloud Computing Sicherheit – Schutzziele. Taxonomie. Marktübersicht., Fraunhofer AISEC, Garching bei München.
29. Triplett, J.E. and Bosworth, B.P. (2006) "Baumol's Disease" has been Cured: IT and Multifactor Productivity in U.S. Services Industries, In: Dennis W. Jansen (Ed.) *The New Economy and Beyond*, Edward Elgar Publishing, Cheltenham, 34-71.
30. Vaquero, L.M., Rodero-Merino, L., Caceres, J. and Lindner, M. (2009) A Break in the Clouds: Towards a Cloud Definition, *ACM SIGCOMM Computer Communication Review*, 39, 1, 50–55.
31. Walsham, G. (1995) Interpretive Case Studies in IS Research: Nature and Method, *European Journal of Information Systems*, 1995, 4, 74–81.
32. White, L.J. (1997) Technological Change, Financial Innovation, and Financial Regulation in the U.S.: The Challenges for Public Policy, *The Wharton Financial Institutions Center Working Papers*, 97, 33.
33. Yin, R.K. (2009) Case Study Research – Design and Methods (4th ed.), Sage Publications, Thousand Oaks.