On the Relevance of Security Risks for Cloud Adoption in the Financial Industry

Completed Research Paper

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

For financial institutions as "heavy users" of Information Technology (IT), the promises of cloud computing – most notably, increased flexibility and reduced provisioning cost – are tempting. However, moving data and applications from a confined internal IT infrastructure to an external, shared cloud poses multiple new security issues. This paper provides an assessment of the relevance of selected issues, based on interviews with 12 representatives of financial institutions. Our results indicate that despite technical advancement and legal arrangements, certain security issues are likely to remain important inhibitors for the adoption of cloud computing by financial institutions.

Keywords

Cloud computing, financial industry, security, risks, problems, relevance, adoption, case study.

INTRODUCTION

Information Technology (IT), in all its facets, has not only massively altered our personal lives in recent decades – just think of smartphones or online social networks – but also substantially transformed the value creation in many industries. This specifically applies for the financial sector, in which the collection, processing, and dissemination of information are the foundation of practically all business processes (Berger, 2003). Hence, across various service industries, the financial sector is among the most intensive users of IT (Triplett and Bosworth, 2006).

However, there are two sides to the role of IT in the financial sector: On the one hand, investments in IT have been empirically shown to yield substantial returns, cost savings, and increases in market share (Brynjolfsson and Hitt, 2000; Ho and Mallick, 2009; Prasad and Harker, 1997). In addition, IT can serve as a driver of innovation, and has historically resulted in products such as online banking or electronic payment (Berger, 2003; Lamberti and Büger, 2009). On the other hand, with IT being an increasingly important production factor, it also constitutes a major expense post. Moormann and Schmidt (2007), for example, estimate that between 15% and 20% of banks' overall administrative expenses can be attributed to IT.

Given the competitive pressure in the financial sector, companies are naturally eager to reduce their IT spending. With *cloud computing*, a new IT paradigm has gained momentum in recent years that promises to facilitate such savings, and has hence raised the interest of IT users. While the term "cloud computing" is somewhat fuzzy, the key idea is to deliver IT services – such as basic compute or storage infrastructure, but also sophisticated applications – as a "utility" via the Internet (Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, Lee, Patterson, Rabkin, Stoica, and Zaharia., 2010; Buyya, Yeo, Venugopal, Broberg, and Brandic, 2009). Due to the exploitation of economies of scale, these services may often be provided cheaper than traditional in-house IT infrastructure (Grossman, 2009). Unfortunately, due to its inherent characteristics, such as virtualization and resource sharing, cloud computing also poses new security challenges (e.g., Armbrust et al., 2010; Grossman, 2009), which may serve as an inhibitor for the adoption of cloud services. This specifically applies for the financial industry, which is among the most heavily regulated industries (White, 1997) and traditionally sensitive to security concerns.

Based on these observations, we examine the following research question: "*To what extent do security concerns pose an obstacle for the adoption of cloud computing in the financial industry?*

In our past work, we have presented a comprehensive overview of potential security risks in cloud computing based on a literature survey (Lampe, Wenge, Müller, and Schaarschmidt, 2012). We further provided the initial results of an ongoing case study within the financial sector, which aims to empirically assess the practical relevance of these issues. In the work at hand, we present updated and additional empirical results from the study, based on interviews with 12 experts from the financial services domain. Our report focuses on an in-depth discussion of selected security risks and can serve as a valuable guideline for both practitioners and researchers in the adoption and scientific examination of cloud computing.

Due to space restrictions, this work does not provide a general introduction into cloud computing. For further details, we refer the interested reader to the seminal works by Armbrust et al. (2010), Buyya et al. (2009), or Mell and Grance (2011).

The remainder of this paper is structured as follows: In the following section, we discuss selected related research in the area of IT and cloud security. Subsequently, we introduce our methodology and present the empirical results that we gathered within our case study. A brief summary of the main findings and an outlook on future work concludes the paper.

RELATED WORK

Since the early days of cloud computing, security risks and problems have been acknowledged as an issue of elevated interest by both practitioners and researchers, and have received substantial attention. In the following, we provide a brief overview of this research domain, with a specific focus on publications that are relevant to the work at hand.

Armbrust et al. (2010) established "data confidentiality/auditability" as one of the top 10 obstacles to 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. Armbrust et al. further outline potential security problems, making the forecast that many issues will be handled through legal agreements, rather than technical solutions.

A comprehensive analysis of security problems in the context of cloud computing has been provided by Ardelt, Dölitzscher, Knahl, and Reich (2011). The authors distinguish between known IT security problems, which are aggravated through cloud computing, and cloud-specific issues. They further analyze the threatened security objectives and propose potential countermeasures.

Streitberger and Ruppel (2009) provide a broad discussion of security in cloud computing. In this context, the authors propose a taxonomy of security aspects, which covers the major domains infrastructure, application and platform, management, and compliance. According to the authors, existing security technologies in the cloud domain lack in maturity, and more sophisticated Service Level Agreements (SLAs) are required to provide adequate security assurances to the users.

Hanna, Mohamed, and Al-Jaroodi (2012) discuss requirements for improved cloud services for governmental, profit and non-profit organizations. The authors' case studies state that archiving, audit, availability, privacy, and security are the most crucial requirements for healthcare providers, financial institutions, and governmental applications. The further requirements considered by Hanna et al. for better cloud services are flexibility, quality of services (QoS), and scalability.

An in-depth analysis of perceived IT security risks (PITSR) in cloud computing has been provided by Ackermann, Widjaja, Benlian, and Buxmann (2012). 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. Furthermore, Ackermann et al. conduct a survey with German companies to validate and evaluate their 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 IT strategy in financial services organizations, Gill, Bunker, and Seltsikas (2011) examine motivators and de-motivators for cloud services adoption based on an empirical survey. The authors identify efficiency, scalability, and future downsize of internal data centers as the main motivators, while lack of maturity, commingling of data in the multitenant environments, and customers regulatory compliance are found as the main de-motivators.

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.

FINDINGS FROM THE FINANCIAL INDUSTRY

Research Methodology

As explained before, we identified 23 potential security problems or risks in cloud computing based on a literature survey in our previous research (Lampe et al., 2012). We aligned these problems with the ten domains of the so-called CISSP certificate, a comprehensive certification that covers diverse areas of IT security, ranging from the physical security of facilities to legal aspects (Conrad, Misenar, and Feldman, 2010; Harris, 2010). In addition, we identified the threatened security objectives, using the well-known "CIA triad" as a basis, which defines confidentiality, integrity, and availability of data as primary concerns (Conrad et al., 2010; Johnson, 2010).

In order to answer the research question, i.e., examine the practical relevance of these issues with respect to the cloud computing adoption in financial institutions, we chose a 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 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 structural guideline for the interviews, we compiled a questionnaire consisting of roughly 40 individual questions. The questionnaire comprises of three sections; 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 IT security, whereas the third part deals with IT compliance.

Using this questionnaire, we conducted interviews with 12 representatives of three companies from the financial services sector. All three companies are headquartered in Germany; two of them have an international business focus, while one company has a stronger focus on the national market. Due to legal constraints, we refrain from providing additional details about the institutes. All interviewees work in the IT department of their respective company; the majority has a professional focus on IT security, and all have experience with cloud computing.

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), 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, as described by Gläser and Laudel (2010). Due to space restrictions, the following report of results focuses on a selected set of security issues, for which we received the most insightful and extensive responses by our interviewees. An overview of these issues is provided in Table 1 on the following page.

Security Problem "Insufficient Security Monitoring Policies"

According to Ardelt et al. (2011), cloud providers should operate a monitoring system, which permits to detect security glitches, take appropriate countermeasures, and inform the clients. However, the authors claim that cloud providers generally do not operate such automated system.

Heinle and Strebel (2010), in contrast, state that some monitoring solutions exist in the area of Infrastructure as a Service (IaaS). However, according to the authors, these solutions are in a state of "infancy" and commonly not compatible or integrated with existing in-house systems. Hence, the security objectives confidentiality, availability, and integrity may be threatened.

According to the interviewees, monitoring systems are widely deployed in the current IT infrastructure. In this context, proactive real-time monitoring is favored over reactive solutions. However, the experts acknowledge that the capabilities of monitoring systems are necessarily limited; according to one interviewee, "monitoring on the level of data records is almost impossible to implement", according to another, "monitoring everything is illusionary". Hence, as one interviewee explained, "[companies] need to trust their employees from some point on".

Table 1: Selected security risks that were examined in our case study. This table is an updated excerpt of a more comprehensive overview, which was provided in our previous work (Lampe et al., 2012).

CISSP Domain	Problem or Risk	Threatened Security Objective[1]	Sources in Alphabetical Order	Respondents/ Codings[2]
Information Security Governance and Risk Management	Insufficient security monitoring policies	C, I, A	Ardelt et al., 2011; Heinle and Strebel, 2010; Hubbard and Sutton, 2010	8 / 22
	Lack of interoperability between cloud service providers	C, I, A	Ardelt et al., 2011[3]; Armbrust et al., 2010; Streitberger and Ruppel, 2009;	10 /29
Access Control	Abuse of administrative privileges or rights	C, I, A	Ardelt et al., 2011; Hubbard and Sutton, 2010	10 / 23
	Abuse or theft of user accounts	C, I, A	Armbrust et al., 2010; Conrad et al., 2010; Hubbard and Sutton, 2010	10 / 29
Business Continuity Planning and Disaster Recovery Planning	Failure of the communication link or data center	A	Armbrust et al., 2010; Conrad et al., 2010	11 / 22
Legal, Regulations, Investigations, and Compliance	Migration of data between different data center locations	C	Ardelt et al., 2011; Streitberger and Ruppel, 2009	11 / 61

With respect to external cloud providers, monitoring is seen as one potential measure amongst many to address security risks. However, as was acknowledged by our respondents, the same restrictions apply as for internal monitoring. In addition, one interviewee highlighted that the monitoring of an external provider would require corresponding legal and technical arrangements.

Security Problem "Lack of Interoperability between Cloud-Service Providers"

Heinle and Strebel (2011) see a lack of technical interfaces as well as incompatible standards as a predominant characteristic of IaaS cloud computing offers. According to the authors, this situation may result in vendor lock-in, i.e., the dependency of a user on a specific provider. Streitberger and Ruppel (2009), as well as Armbrust et al. (2010), share this concern, where the latter more specifically refer to it as the risk of "data lock-in".

According to Ardelt et al. (2011), the incompatibility between different cloud providers is problematic with respect to the security objective of availability. In our opinion, a lack of interoperability may further threaten the objectives of confidentiality and integrity, because a potentially insecure and error-prone conversion process is required once data is moved into or out of an external cloud, respectively between different clouds.

With respect to this issue, our study revealed controversial standpoints among the interviewees. Some respondents claimed that a lock-in effect due to insufficient interoperability should not occur in a market with highly standardized services, and claimed that individual vendors would not be able to lock-in their customers in the long run. In this context, one interviewee claimed an ongoing convergence in the cloud computing market with respect to services and prices, which would render individual providers exchangeable – like a "cellular provider" – in the future.

Other interviewees, however, referred to the risk of vendor lock-in as a "fundamental inhibitor" for the adoption of cloud computing in the financial sector; another interviewee specifically called it "a very large risk today". According to one interviewee, the risk of vendor lock-in specifically persists in the public cloud, where the user only retains control of "very small segments [of the overall IT infrastructure]".

[1] Abbreviations: Confidentiality (C), Integrity (I), and Availability (A). Please refer to Johnson (2010) for a definition.

[2] Number of interviewees that made statements about a specific issue and corresponding number of *codings*, i.e., interview transcript fragments that were considered in the analysis.

[3] Please note that we incorrectly listed Hubbard and Sutton (2011) instead of Streitberger and Ruppel (2009) as source for this specific security problem in our previous publication.

Security Problem "Abuse of Administrative Privileges or Rights"

Hubbard and Sutton (2011) state that the abuse of privileges or rights through malicious insiders is a well-known problem in IT, which, however, is aggravated with the introduction of cloud computing. In this respect, the authors see the lack of transparency as the key deficit within cloud computing, because cloud providers do not, e.g., disclose their hiring or monitoring policies. Conrad et al. (2010) further point out that insider attacks are not necessarily intentional, but may also result from mistakes that are made due to insufficient training.

This is specifically problematic in the context of IaaS, where users lease virtual machine instances, and external administrators commonly have root access to the underlying host machines. Thus, through the so-called hypervisor, i.e., the virtualization software, external parties may access the client machines, and hence, client data (Ardelt et al., 2011). Thus, this problem potentially threatens all considered security objectives, namely, confidentiality, availability, and integrity.

In accordance, this potential security problem is seen as a "valid scenario" with "a massive potential for abuse" by the respondents in our case study. Hence, the interviewees agreed that external parties and their staff members need to underlie the same stringent control systems as internal employees. Thus may involve measures such as a preliminary background screening or constant monitoring for suspicious activities.

However, the respondents also stated that while such procedures may be negotiated with a cloud provider, their correct implementation cannot be fully controlled by the cloud user. In accordance, one interviewee argued that "highly sensitive data cannot be outsourced". Another stated that retaining control of the encryption keys may provide a viable solution, which would prevent the access of malicious insiders to encrypted data.

Security Problem "Abuse or Theft of User Accounts"

According to Hubbard and Sutton (2010), the "hijacking" of accounts, based on attack methods such as "phishing, fraud, and exploitation of software vulnerabilities", is a well-known problem in IT systems. It may target large user groups, but also "high-value" individuals, such as executives (Conrad et al., 2010).

While the theft of user accounts is not a new phenomenon, the use of external cloud providers adds a new attack vector: As Hubbard and Sutton (2010) further explain, an attacker may not only, e.g., gain access to confidential information, but also exploit the illegal access for future attacks on third parties. Hence, the abuse or theft of user accounts threatens all three considered security objectives, i.e., confidentiality, availability, and integrity.

Most of the interviewees in our study acknowledged that the abuse or theft of user accounts is a practical risk in cloud computing; one interviewee characterized it as "inherent risk". Another interviewee pointed out that the provision of IT services in general involves multiple external providers. Correspondingly, he argued that "service providers have to be incorporated into the [internal] security measures".

As an example of an actual (technical) measure, one interviewee named "certificate-based authentication". Other interviewees more generally stressed the role of "appropriate processes" for the minimization of security risks. Three respondents further stated that it is important for a company to raise awareness among employees concerning the potential abuse of administrative privileges. This may be accomplished through educational measures.

Security Problem "Failure of the Communication Link or Data Center"

According to the seminal work by Armbrust et al. (2010), service availability – or more precisely, a lack thereof – is among the top obstacles for the adoption of cloud computing. The authors argue that despite geographically distributed data centers, an individual cloud provider may constitute a "single point of failure", e.g., due to the use of the identical software or the risk of bankruptcy, which is undesirable in high-availability scenarios.

Conrad et al. (2010) provide various examples for so-called "disruptive events" that may result in the outage of a communication link or data center. These events range from natural catastrophes, such as hurricanes, to acts of terrorism. In our opinion, such events primarily constitute a threat to the security objective of availability.

According to our interviewees, dedicated private communication lines are generally preferred over public networks, such as the Internet. The handling of communication outages is perceived as a matter of proper legal arrangements with the respective providers; however, technical solutions, i.e., redundant lines, are also required in the case that "a network provider is not able to deliver its service". Nevertheless, one interviewee acknowledged that "general outages of the Internet [..] cannot be compensated", saying that such scenario was "out of our control sphere".

In order to address data center outages, the institutes in our study generally pursue a mirroring strategy, which involves pairs of similar data centers and permanent replication of data. The efficiency of these strategies is verified through continuous simulation and internal auditing procedures. The same requirements as for the internal IT infrastructure would likely apply for external clouds. As one interviewee put it, "a cloud scenario would require the practical ability to replace a data center", specifically in the case of critical data.

Security Problem "Migration of Data between Different Data Center Locations"

As Ardelt et al. (2011) explain, the uncertainty concerning the physical location of data is one of the main differences between traditional IT outsourcing and cloud computing. Due to lack of appropriate monitoring mechanisms, data may be moved between data centers in different geographical areas, and cloud users may subsequently get in conflict with data privacy laws or regulatory requirements.

According to Streitberger and Ruppel (2009), such legal or regulatory requirements may, for example, apply to finance-related data such as tax information. The authors further explain that the security objective of confidentiality may easily be hurt if a cloud provider has the right to "read, disclose, or transfer" data, given that the applicable laws substantially differ between different geographical regions and corresponding jurisdictions.

The participants of our case study acknowledge that the potential migration of data between data centers and resulting uncertainty about its physical whereabouts can be problematic. According to our respondents, data is generally classified according to the applicable regulatory requirements.

Based on this classification, the physical location may be restricted to certain "perimeters". In the case of the Germany-based companies in our case study, these perimeters involve Germany, the European Union (EU), and so-called (unsafe) third countries. In this context, the *Safe Harbor* agreement – with permits to transfer sensitive data from the EU to the United States under certain conditions (Streitberger and Ruppel, 2009) – is seen as "insufficient", because "American authorities have comprehensive [data] access rights in the case of legal investigations". Nevertheless, in general, legal agreements with cloud providers are perceived as a viable option to regulate and restrict the migration of data.

CONCLUSIONS AND OUTLOOK

For the financial industry as an intensive user of IT, cloud computing offers a large potential for cost savings. However, given that the financial sector is a heavily regulated industry that deals with valuable and sensitive information, security issues may pose a major inhibitor for cloud adoption.

Our past research, which featured an extensive literature survey, has indicated that cloud computing, specifically based on a public cloud deployment model, poses a variety of security problems (Lampe et al, 2012). Some of these issues have already been examined in the IT security domain in the past, while others newly arise due to the inherent characteristics of cloud computing, such as the common use of virtualization and multi-tenancy.

On the basis of the 12 personal interviews that we have conducted with representatives from the financial industry, it can be concluded that most of these problems do, in fact, serve as inhibitors to cloud adoption. Yet, the practical relevance and individual assessment of these problems substantially differs.

To start with, in the area of security monitoring, adequate solutions appear to exist today, even though they have their limitations. The key challenge for financial institutions as prospective cloud users exists in putting those mechanisms in place at external cloud providers; this is a legal, rather than technical challenge. Yet, it may still be difficult to tackle, because today's public clouds very much profit economically from their minimum of service individualization.

Insufficient interoperability among providers is a strongly disputed issue. At the time being, it is difficult to judge whether this concern will be resolved through standardization efforts. Yet, at least in the IaaS area, some progress has been made in recent years, and despite some perceptions, even providers may ultimately benefit from the process (Armbrust et al., 2010).

Both the abuse of administrative rights and stolen user accounts are well-known challenges, but may further gain in relevance in cloud computing scenarios. Our study indicates that the corresponding security concerns can partially be resolved by technical measures and legal agreements. However, specifically the issue of abuse of administrative rights could be a major inhibitor for financial institutions to adopt public cloud services unless providers are willing to act more transparently.

With respect to hardware failures, it will be interesting to see whether public cloud providers are willing and able to offer the same availability standards that are enforced in private IT infrastructures today. If not, applications of the public cloud will

likely be limited to non-critical data and business applications in the future, thus serving as a (limited) complement to existing internal IT.

Lastly, the migration of data and resulting unawareness of its physical location – according to the National Institute of Standards and Technology (NIST), one of the essential characteristics of cloud computing (Mell and Grance, 2011) – remains a severe challenge. Specifically for European banks, which underlie strict legal and regulatory requirements, the potential exposure of data to foreign authorities poses a major inhibitor for cloud adoption. Yet, the tendency of public cloud providers to construct dedicated data centers in different jurisdictions may alleviate these concerns in the medium- and long-term.

In summary, with respect to our initial research question from the introduction, it can be concluded that security concerns do pose an important inhibitor for the adoption of cloud computing in the financial services sector. In addition, our case study indicates that despite technical advancements, many of these issues will remain challenging in the medium- and long-term. Hence, it is safe to conclude that financial institutions will continue to provide large parts of their required IT capacities in-house in the future, rather than purchase them from external (public) cloud providers.

In our future work, we primarily aim to complement our current qualitative research approach through a larger scale quantitative study, which will permit more a statistically sound assessment of security problems in the cloud computing domain. In addition, our research focus lies on the development of technical solutions to address those risks that were identified as main inhibitors for cloud adoption in this paper.

ACKNOWLEDGEMENTS

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

REFERENCES

1. Ackermann, T., Widjaja, T., Benlian, A., Buxmann, P. (2012) Perceived IT Security Risks of Cloud Computing: Conceptualization and Scale Development, In *Proceedings of International Conference on Information Systems*, December 16-19, Orlando, United States.
2. 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.*
3. 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.
4. 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.
5. 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.
6. 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.
7. Carroll, M., van der Merwe, A., Kotze, P. (2011), Secure Cloud Computing: Benefits, Risks and Controls, In *Proceedings of the Information Security South Africa*, August 15-17, Johannesburg, South Africa, 1-9.
8. Conrad, E., Misenar, S. and Feldman, J. (2010) CISSP Study Guide, Elsevier, Burlington.
9. Gill, A.Q. and Bunker, D., 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*, December 12-14, Sydney, Australia, 697-704.
10. Gläser, J. and Laudel, G. (2010) Experteninterviews und qualitative Inhaltsanalyse (4th ed.), VS Verlag, Wiesbaden.
11. Grossman, R.L. (2009) The Case for Cloud Computing, *IT Professional*, 2, 11, *23-27.*
12. Hanna, E.M., Mohamed, N. and Al-Jaroodi, J. (2012) The Cloud: Requirements for a Better Service, In *Proceedings of the 2012 IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, May 13-16, Ottawa, 787–792.
13. Harris, S. (2010) CISSP Certification All-in-One Exam Guide (5th ed.), McGraw-Hill, New York.
14. 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*, August 30-31, Ischia, Italy, 93-104.

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. Johnson, B.C. (2010) Information Security Basics, *ISSA Journal*, 8, 7, 28-32.
18. 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.
19. Lampe, U., Wenge, O., Müller, A., Schaarschmidt, R. (2012) Cloud Computing in the Financial Industry – A Road Paved with Security Pitfalls? *Proceedings of the 18th Americas Conference on Information Systems*, August 9-11, Seattle, United States, 1-11.
20. 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
21. Moormann, J. and Schmidt, G. (2007) IT in der Finanzbranche, Springer-Verlag, Berlin / Heidelberg.
22. 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.
23. Streitberger, W. and Ruppel A. (2009) Cloud Computing Sicherheit – Schutzziele. Taxonomie. Marktübersicht., Fraunhofer AISEC, Garching bei München.
24. 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.
25. Walsham, G. (1995) Interpretive Case Studies in IS Research: Nature and Method, *European Journal of Information Systems*, 1995, 4, 74–81.
26. 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.
27. Yin, R.K. (2009) Case Study Research – Design and Methods (4th ed.), Sage Publications, Thousand Oaks.