Research Report

Security Risks in Cloud Adoption – A Study in the Financial Industry

WHILE CLOUD COMPUTING PROMISES COST SAVINGS, IT ALSO POSES A VARIETY OF POTENTIAL SECURITY ISSUES. BASED ON INTERVIEWS WITH 12 EXPERTS FROM THE FINANCIAL INDUSTRY, WE ASSESS THE PRACTICAL RELEVANCE OF SELECTED SECURITY PROBLEMS FOR CLOUD ADOPTION IN THAT SECTOR.

Ulrich Lampe
Alexander Müller
Olga Wenge
Ralf Schaarschmidt*

Introduction

IT is undoubtedly among the most important production factors in the financial industry, given that the processing of information is the key element of practically all business processes in the regarded sector. At the same time, IT also constitutes a substantial expense post.

Given these aspects, cloud computing has recently raised the interest of companies in the financial sector. This paradigm promises to reduce IT spending through characteristics such as self-service, scalability, and pay-per-use pricing schemes.

However, our previous research has shown that cloud computing is also associated with a large number of potential security problems (Lampe et al., 2012). Given the legal requirements and regulatory pressure that the financial sector is facing and the sensitivity of the data it operates on, these security issues may pose significant obstacles to cloud adoption.

In our work, we assess the relevance of selected security issues through a case study, based on interviews with multiple representatives from the financial industry. Accordingly, our leading research question is: *"To what extent do security concerns pose an obstacle for the adoption of cloud computing in the financial industry?"*

Methodology

We identified 23 potential security problems or risks in cloud computing based on a literature survey in our previous research (Lampe et al., 2012). Subsequently, we structured these problems using the ten domains of the so-called CISSP (Certified Information Systems Security Professional) certificate, a comprehensive certification that covers diverse areas of IT security, ranging from the physical security of facilities to legal aspects (Conrad et al., 2010; Harris, 2010). Furthermore, for each problem, we identified the threatened security objectives using the classic "CIA triad" as a basis. It defines confidentiality (C), integrity (I), and availability (A) of data as primary concerns (Conrad et al., 2010).

In order to empirically answer our research questions, i.e., assess the relevance of the previously identified security problems, we chose the qualitative instrument of a case study. As primary data source, we selected personal interviews. While this instrument does not permit for statistical analysis of data and requires careful interpretation, it allows a targeted examination of a specific topic, and hence potentially more insights than a purely quantitative approach. As guideline for the interviews, we compiled a questionnaire consisting of approximately 40 items.

Based on this questionnaire, we conducted a series of 12 interviews with representatives of three German financial services companies. Two of these companies act in the international market, while one company is more focused on the national market. Each interview lasted approximately one hour, was digitally recorded, and subsequently transcribed into written text. Given the sensitive nature of our research, we allowed for a subsequent editing and authorization step by the interviewees. The authorized transcripts were then analyzed using the method of *qualitative content analysis* (Gläser and Laudel, 2010).

Study Results

Due to space restrictions, we focus on a selected set of six security issues, for which we received the most extensive and insightful answers. An overview is provided in Table 1. For each issue, we briefly explain its significance and present the key findings of our study. A more extensive presentation can be found in our recent conference paper (Lampe et al., 2013).

Findings concerning "Insufficient Security Monitoring Policies"

Monitoring systems are seen as an important instrument to detect security glitches and take appropriate countermeasures. However, such mechanisms are seen as non-existent or rudimentary and poorly interoperable in the cloud computing domain (Ardelt et al., 2011; Heinle and Strebel, 2010). Due to this situation, the security objectives confidentiality, availability, and integrity may be threatened by cloud adoption.

According to our interview partners, monitoring solutions – preferably proactive, rather than reactive ones – are widely deployed within the existing IT infrastructure of the respective institutes. However, their capabilities are limited; as one interviewee put it, "monitoring everything is illusionary", and hence, another

* IBM Global Business Services

explained, "[companies] need to trust their employees from some point on".

Concerning external cloud providers, monitoring is perceived as a suitable instrument to address security risks. However, as pointed out by our interviewees, this would require corresponding legal and technical arrangements with the cloud provider. In addition, for external cloud computing, the same limitations with respect to monitoring – e.g., the inability to monitor on the level of individual data records – apply as for internal IT.

Findings concerning "Lack of Interoperability between Cloud Service Providers"

Various authors have previously identified the lack of interoperability among providers, resulting in the risk of provider lock-in or data lock-in, as one of the key obstacles for cloud adoption (Armbrust et al., 2010; Heinle and Strebel, 2010; Streitberger and Ruppel, 2009). While this risk only threatens the objective of availability upon first sight, it may – in our opinion – also endanger data integrity and confidentiality due to the need for a conversion or migration processes, which may potentially be error-prone and insecure.

CISSP Domain	Problem or Risk	Threatened Security Objective	Sources
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
	Lack of interoperability between cloud service providers	C, I, A	Ardelt et al., 2011; Armbrust et al., 2010; Streitberger and Ruppel, 2009
Access Control	Abuse of administrative privileges or rights	C, I, A	Ardelt et al., 2011; Hubbard and Sutton, 2010
	Abuse or theft of user accounts	C, I, A	Armbrust et al., 2010; Conrad et al., 2010; Hubbard and Sutton, 2010
Business Continuity Planning and Disaster Recovery Planning	Failure of the communication link or data center	A	Armbrust et al., 2010; Conrad et al., 2010
Legal, Regulations, Investigations, and Compliance	Migration of data between different data center locations	C	Ardelt et al., 2011; Streitberger and Ruppel, 2009

Table 1: Overview of considered security problems that were examined in our study (Abbreviations: C – Confidentiality; I – Integrity; A – Availability)

Concerning this issue, we received highly controversial statements in our study. Some respondents claimed that services are becoming increasingly standardized, leading to improved interoperability and thus the inability of cloud providers to lock in their customers. One interviewee explicitly noted an ongoing convergence process in the cloud market, saying that individual providers would soon be exchangeable, similar to "cellular providers" today.

In contrast, another group of respondents saw the risk of lock-in as "fundamental inhibitor" for cloud adoption, specifically in public clouds where users only control "very small segments [of the overall IT infrastructure]".

Findings concerning "Abuse of Administrative Privileges or Rights"

While the abuse of administrative privileges has been a well-known security problem for many years, it is aggravated in cloud computing, most notably due to a lack of transparency concerning the hiring or monitoring policies of services providers (Hubbard and Sutton, 2010). The problem specifically applies for infrastructure services, where cloud administrators may gain access to virtual machines and data residing on them (Ardelt et al., 2011), thus threatening all three aforementioned security objectives.

Our respondents saw the abuse of administrative privileges as a "valid scenario" with "a massive potential for abuse". Hence, external parties and their staff members would have to be subjected to the same control systems, involving measures such as background screening, as internal employees.

At the same time, our respondents acknowledged that while such procedures may be legally negotiated, their correct implementation could not be fully validated. Based on that notion, one interviewee said that "highly sensitive data cannot be outsourced". However, the use of encryption and exclusive ownership of the corresponding encryption keys may provide a technical solution to prevent abuse.

Findings concerning "Abuse or Theft of User Accounts"

Theft of user accounts has grown into a considerable problem in recent years, e.g., based on attack methods, such as phishing or the exploitation of software vulnerabilities (Hubbard and Sutton, 2010). While the problem is not exclusive to cloud computing, this paradigm opens additional attack vectors and brings new risks, such as the exploitation of cloud resources for attacks on third parties (Hubbard and Sutton, 2010). As can easily be reasoned, the abuse or theft of user accounts threatens all three considered security objectives, i.e., confidentiality, integrity, and availability.

Most interviewees in our study judged the abuse of user accounts as practical or even "inherent" risk. Hence, as similarly proposed for the previous issue of administrative privilege abuse, one respondent argued that "service providers have to be incorporated into the [internal] security measures".

As potential countermeasures, "certificatebased authentication" was proposed, and the importance of "appropriate processes" was stressed. This specifically includes training measures among employees to raise awareness for attacks that target user credentials.

Findings concerning "Failure of the Communication Link or Data Center"

A lack of service availability is considered among the top obstacles for cloud adoption by Armbrust et al. (2010). Service outages have various reasons, ranging from software bugs to natural catastrophes (Conrad et al. 2010). Specifically, the former may not be restricted to individual data centers, but may concern all services of a cloud provider.

Our interviewees explained that – despite the perception that cloud computing mostly relies on public networks – private communication lines are preferred. Hence, handling of outages is primarily addressed through legal arrangements. However, technical measures, such as redundant lines, also come into play.

In the current IT infrastructure, mirroring strategies are applied for data centers, with these measures being constantly verified through simulation and auditing. Hence, a cloud-based infrastructure would have to provide for similar redundancy, with one respondent explicitly saying that "a cloud scenario would require the practical ability to replace a data center".

Findings concerning "Migration of Data between Different Data Center Locations"

Ardelt et al. (2011) identify the uncertainty concerning the physical location of data as main difference between traditional IT outsourcing and cloud computing. In (public) clouds, data is potentially moved between different data centers and hence jurisdictions. Thus, cloud users may violate legal or regulatory requirements, specifically when sensitive data – such as prevalent in the financial industry – is concerned. Depending on the applicable laws, authorities may gain access to the data and threat its confidentiality.

The participants of our study perceive the potential migration of data between physical locations as problematic. In general, data is classified according to the applicable regulatory requirements, resulting in three perimeters, namely Germany, the European Union (EU), and (unsafe) third countries. Accordingly, data has to reside within the matching physical locations. In this context, the safe harbor agreement – which permits data transfer to the United States under certain conditions – is seen as insufficient, because "American authorities have comprehensive [data] access rights in the case of legal investigations". However, legal agreements are generally perceived as suitable means to ensure data safety.

Summary

In conclusion, with respect to our initially stated research question, our case study confirms that security problems pose an important obstacle for cloud adoption. While some of these issues may be resolved through technical measures, such as the use of more sophisticated authentication mechanisms or monitoring solutions, others – most notably uncertainty about data location – will likely remain challenging in the future, since they result from the inherent properties of cloud computing. Hence, we believe that a focus of financial service companies will remain on the adoption of internal, private clouds in the future, potentially complemented by the use of public clouds for less security-sensitive applications.

References

Ardelt, M.; Dölitzscher, F.; Knahl, M.; Reich, C.:
Sicherheitsprobleme für IT-Outsourcing durch Cloud Computing.
In: HMD – Praxis der Wirtschaftsinformatik, 48 (2011) 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.; Zaharia, M.:
A View of Cloud Computing.
In: Communications of the ACM, 53 (2010) 4, pp. 50-58.

Conrad, E.; Misenar, S.; Feldman, J.:
CISSP Study Guide, Elsevier, Burlington, 2010.

Gläser, J.; Laudel, G.:
Experteninterviews und qualitative Inhaltsanalyse (4th ed.), VS Verlag, Wiesbaden, 2010.

Harris, S.:
CISSP Certification All-in-One Exam Guide (5th ed.), McGraw-Hill, New York, 2010.

Heinle, C.; Strebel, J.:
IaaS Adoption Determinants in Enterprises.
In: Proceedings of the 7th International Conference on Economics of Grids, Clouds, Systems, and Service, Ischia, Italy, 2010.

Hubbard, D.; Sutton, M.:
Top Threats to Cloud Computing V1.0.
Available online at *https://cloudsecurityalliance.org/topthreats/ csathreats.v1.0.pdf*, 2010.

Lampe, U.; Wenge, O.; Müller, A.; Schaarschmidt, R.:
Cloud Computing in the Financial Industry – A Road Paved with Security Pitfalls?
In: Proceedings of the 18th Americas Conference on Information Systems, Seattle, WA, United States, 2012.

Lampe, U.; Wenge, O.; Müller, A.; Schaarschmidt, R.:
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, United States, 2013.

Streitberger, W.; Ruppel A.:
Cloud Computing Sicherheit – Schutzziele. Taxonomie. Marktübersicht., Fraunhofer AISEC, Garching bei München, 2009.