ISSN 2277-3061

The use of cloud technology in Corporate Information Systems

Rufat F. Talibov
"Information Technology and Programming" department
Azerbaijan Technical University, Azerbaijan, Baku
“Delta Telecom LTD” Chief Engineer of Data Center
r.talibov@delta-telecom.net
Zafar Jafarov
"Information Technology and Programming" department
Azerbaijan Technical University, Azerbaijan, Baku
c.zafar@mail.ru

ABSTRACT

For automation 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 for automation industry prospectively. However, given the high degree of regulation, concerns regarding security and compliance requirements arise. In this work, provide a theoretical analysis of 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 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

Industrial systems; automation industry; cloud technology; security compliance

Council for Innovative Research

Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Vol. 14, No. 1

www.ijctonline.com , editorijctonline@gmail.com

ISSN 2277-3061

1. INTRODUCTION

For automation industry, the collection, processing, and dissemination of large amounts of information constitute the basis for all processes [1]. Accordingly, industry institutions are among the most intensive users of Information Technology (IT) across various service industries. Following some controversy about the “productivity paradox” of IT in the, it has been empirically validated since that investments in IT may result in substantial returns, cost savings. Due to the constant decline in the absolute cost of IT equipment, many industry 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. As a result, IT constitutes a major expense post for most industrial institutions today.

Lately, cloud computing has arrived as a novel IT paradigm that promises to “revolutionize” the way IT services are provisioned and consumed. The essential idea of cloud computing is to deliver IT services – such as compute infrastructure or storage – in a utility-like manner , thus making these services ultimately more flexible and cost-efficient. Given the role of IT in the critical infrastructure industrial , as an essential production factor, but also a major expense post, cloud computing may seem as a “perfect match” for this industry [2].

However, there appears to be one major obstacle: security. In fact, analysis confirmed that general security concerns and data privacy concerns constitute the most severe reasons for not using cloud computing. It is reasonable to conclude that these concerns are especially pronounced in the critical infrastructure, which is among the most regulated sectors, and thus subject to rigid security requirements.

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 critical infrastructure industry and, if yes, which concerns specifically”? We provide a theoretical analysis of potential security problems in conjunction with the application of cloud computing.

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, analyse potential security with the use of cloud computing in the industrial systems. Thereafter, we present the methodology and results of our ongoing empirical research. The paper concludes with a brief summary and outlook.

2. A BRIEF OVERVIEW OF THE CONCEPT OF CLOUD TECHNOLOGY

While the term cloud computing is currently very popular in research and practice today, no commonly accepted definition exists so far. 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”. Such resources may include virtually any type of computing capabilities, including “networks, servers, storage, applications, and services”. 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). A basic taxonomy is cloud systems, which distinguishes four common deployment and three service models [3]. An overview is depicted in Figure 1. 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 [5].

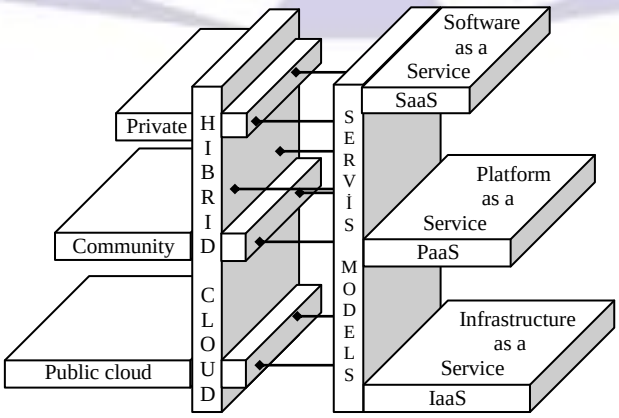

Figure 1: Common cloud deployment and service models

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. In general, the complexity of the services increases moving from IaaS to SaaS, whereas the degree of (technical) standardization appears to decrease [6].

3. SECURITY PROBLEMS FOR CLOUD TECHNOLOGY

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 analysis, used the ten security domains of the well-known Certified Information Systems Security Professional (CISSP) certificate [7]. 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. Most of these domains can be found in identical or comparable form in other IT security guides, e.g., by the Cloud Security Alliance or the Information Systems Audit and Control Association. 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, mapped each security problem or risk that found in the literature onto one of the ten CISSP domains. In addition, 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“. 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 [8]. Lastly, availability means that information or a system is accessible in a timely and reliable way whenever needed.

4. EMPIRICAL ANALYSIS IN THE INDUSTRY SYSTEMS

A. Methodology

In order to empirically assess our research question and examine the practical significance of the previously identified, cloud computing-related security issues, 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. In work, pursue a holistic, multi-case design. In this context, holistic means that industry institutions as a whole – and not their individual units or departments – constitute the matter of examination. Chosen a multi-case design due to the potentially higher robustness and explanatory power of such design. As primary data source, 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.

As the basis for the interviews, compiled a questionnaire consisting of roughly 40 individual questions. Using this questionnaire, conducted interview with two representatives of a industry institutions Azerbaijan. 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.

The transcripts and notes were analyzed using the method of qualitative content analysis. 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. In contrast to more complex analysis procedures, such as the coding method, the qualitative content analysis requires less initial effort and is thus [9]. very well suited for the deduction of preliminary results

B. Preliminary Results

The entire document should be in Times New Roman or Times font. Type 3 fonts must not be used. Other font types may be used if needed for special purposes.

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 industry, the discussion of results focuses on the critical infrastructure. However, initial results can provide valuable insights with respect to the research question [10].

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 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 automation industry. However, according to the interviewees, cloud computing will not be the dominant delivery model in any critical infrastructure, because some processes cannot be outsourced to third parties. Automation industry 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 critical infrastructure itself or its outsourced partners. According to both interviewees, IT in the critical infrastructure 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 critical infrastructure industry. Still, critical infrastructure should be very aware about the dependence on specific vendors.

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 interviewees 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 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 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” 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 critical infrastructure 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.

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 critical infrastructure tend to use the instrument of legal agreements and compliance rules to mitigate risks and shift the financial and legal responsibility for security issues to the cloud providers.

5. CONCLUSIONS

In the automation 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 industrial systems. However, security concerns have recently been named as a potential sticking point for the adoption of cloud computing, specifically in the critical infrastructure which is subject to a multitude of regulatory requirements.

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

According to the interviews with two experts, 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 critical infrastructure in the industry area.

On the basis of the case study analysis, it appears that critical infrastructures 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.

REFERENCES

[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] 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.

[4] 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.

[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] 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.

[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.