CLOUD COMPUTING AND INFORMATION SECURITY

Jan Čapek

Abstract: *The article takes into account cloud computing and information security. It is shown, that in spite of the advantage from costs point of view the data - placed within the cloud are still not safe, due to the fact that providers are not able to secure data from physical point of view. So the customers have not physical control of theirs data. Existing standard activities cloud for data security does not solve this problem yet.*

Keywords: *Information security, Cloud computing, Threads, Services, Cloud security.*

JEL Classification: *D80, D89.*

Introduction

Information security is a comprehensive approach to information protection as a whole. It is therefore important to protect information in all its forms and throughout their life cycle - i.e. during their formation, processing, storage, transfer and disposal. For effective protection, it is necessary to determine what information the organization has and what value it should. Management of the organizations must identify objectives and real-world performance of their organization and only on the basis that require effective information security management system. It should be noted that the aim is not just implementation, but also other long term development and functiona lity of the system in a response to changes in the organization and its environment. [3] One of the definitions of cloud computing says "Cloud computing is a method of approach to the use of computer technology, which is based on the provision of shared computing resources and their use as a service". There are various service models and options for delivery, but all types of cloud computing is the ability to provide shared resources on demand, elastic, self-service and through an extensive network of access and the ability to measure the consumed service in shared resource pool.

1 Statement of a problem

Cloud computing is marketing term that refers to web-based application, storage, and communications services. In cloud computing [11], a data centre holds information that end-users would more traditionally have stored on their computers. This raises concerns regarding user privacy protection because users must outsource their data. Additionally, the move to centralized services could affect the privacy and security of users' interactions. Security threats might happen in resource provisioning and during distributed application execution. Also, new threats are likely to emerge. For instance, hackers can use the virtualized infrastructure as a launching pad for new attacks. Cloud services should preserve data integrity and user privacy. At the same time, they should enhance interoperability across multiple cloud service providers. In this context, we must investigate new data-protection mechanisms to secure data privacy, resource security, and content copyrights.

In a sense, what we're seeing now is the second coming of cloud computing. Almost 50 years ago a similar transformation came with the creation of service bureaus and time-sharing systems that provided access to computing machinery for users who lacked a mainframe in a glass-walled room down the hall. A typical time-sharing service had a hub-and-spoke configuration. Individual users at terminals communicated over telephone lines with a central site where all the computing was done.

When personal computers arrived in the 1980s, part of their appeal was the promise of "liberating" programs and data from the central computing centre. Individuals were free to control their own computing environment, choosing software to suit their needs and customizing systems to their tastes. But PCs in isolation had an obvious weakness: In many cases the sneaker net was the primary means of collaboration and sharing. The client-server model introduced in the 1980s offered a central repository for shared data while personal computers and workstations replaced terminals, allowing individuals to run programs locally.

Management of firms with information security is connected by two bonds. The first link is the marketing. If a company increases its credibility in the market through certification of its quality assurance system should also expect an audit query security information. The second link is a link from the inseparability of information management and the business processes themselves. Business information is known to its own source, like the staff or money. Insecurity threatens the production of own resources and thus leads to an increase risk for the company itself and the rapid spread of threats the surrounding commercial environment. Information security has thus undoubtedly crucial for companies that sell it as part of its production. For example, software, legal, consulting and / or reporting companies even sell it as their main commodity. [2]

2 Methods

In this section, a review of literature, limited mainly to academic articles and recent books are presented. First, searching for articles dealing with cloud computing in general was made. Regarding the fact that objective of this paper is the discussion about data security during cloud techniques using. The final searching area involved security information, where again general literature was used. As the methods the analysis and comparison was used. The article is organised as follows: The first part is dedicated to cloud computing with divide into two subchapters cloud infrastructure and cloud services. The second part is dedicates to Information security within cloud computing.

2.1 Related works

Nowadays a plenty of articles exist in which the cloud computing and/or information security or both are covered. For example [9] the security best practices for cloud computing created by Cloud Security Alliance (CSA). The best practices in designing for the cloud was discussed in [10]. Nice overview article can be found in [11] Cloud Standards is an aggregation site chronicling the progress of several organizations that develop the technological standards for the architecture, control and

security of clouds are discussed in [12]. The Open Web Application Security Project (OWASP) is a not-for-profit organization that develops security software for application testing. OWASP is concerned with Internet and cloud technologies because these areas of study contain myriad application-level vulnerabilities, which are poorly understood by the people who deploy web applications [13].

3 Cloud computing

Cloud computing is at the heart of many pragmatic organizations which dislike the increasing complexity and inflexibility of their IT environment and rising operation costs. Cloud computing is attractive for them because it brings the promise of much simpler and more efficient deployment and management of IT. According [14] is possible divide the cloud into two main groups as follow:

1. **The Internal Cloud.** This is, in many ways, the most common type of cloud computing. The internal cloud occurs within a single organization, allowing them to implement virtualization for in-house services. The premise is that internal infrastructure including server, networks, storage and applications will be connected and virtualized, which in turn allows it to move things around in such a way as to maximize efficiency. This is different from a simply virtualized situation in that it allows a higher degree of automation and even a chargeback capability for the other business units.
2. **External Cloud Hosting.** This type of cloud model uses an external service via a cloud provider, and its access by the organization via the Internet. This is probably the most cost-effective way to utilize the cloud. The big concern with this model, of course, is security. Performance is also a concern, in many quarters.

The **External Cloud Hosting** can be divided into four following cloud computing deployment models [15]

A. Public Cloud. The traditional mainstream sense of cloud computing. The cloud is made available to the general public or a large industry group and is owned by an organization providing cloud services. Resources are provisioned from an off-site third-party provider who shares resources.

B. Private Cloud. The cloud is operated exclusively for an organization. It may be managed by the organization or a third party and may exist on premise or off premise

C. Hybrid Cloud. The cloud infrastructure is a composition of two or more clouds that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability. The environment is consisting of multiple internal and/or external providers.

D. Community Cloud. The cloud infrastructure is shared by several organizations. It may be managed by the organizations or a third party and may exist on premise or off premise.

3.1 Cloud Infrastructure

It is an infrastructure necessary to provide (usually transparent) cloud services to users. Itincludes features for virtualization and federation funds standardize and autom

ate operations processes, user access to computer service and to choose the quality and quantity of services consumed, and finally the method of measuring and billing of services rendered.

One can assume according to [16] that the customer's revenue is directly proportional to the total number of user-hours (UH). This assumption is consistent with the ad-supported revenue model in which the number of ads served is roughly proportional to the total visit time spent by end users on the service.

$$\text{UH}_{cloud} \times (revenue - Cost_{cloud}) \geq UH_{datacenter} \times \left(renevue - \frac{Cost_{datacenter}}{Utilization}\right) \quad (1)$$

The left-hand side multiplies the net revenue per user-hour (revenue realized per user-hour minus cost of paying Cloud Computing per user-hour) by the number of user-hours, giving the expected profit from using Cloud Computing. The right-hand side performs the same calculation for a fixed-capacity datacentre by factoring in the average utilization, including nonpeak workloads. Whichever side is greater represents the opportunity for higher profit.

3.2 Cloud Services

Cloud services can be divided into:

1. Infrastructure services in the cloud computing environment to ensure compliance with requirements laid down in the agreement on service level (such as performance, availability, and data storage, and security, capacity)

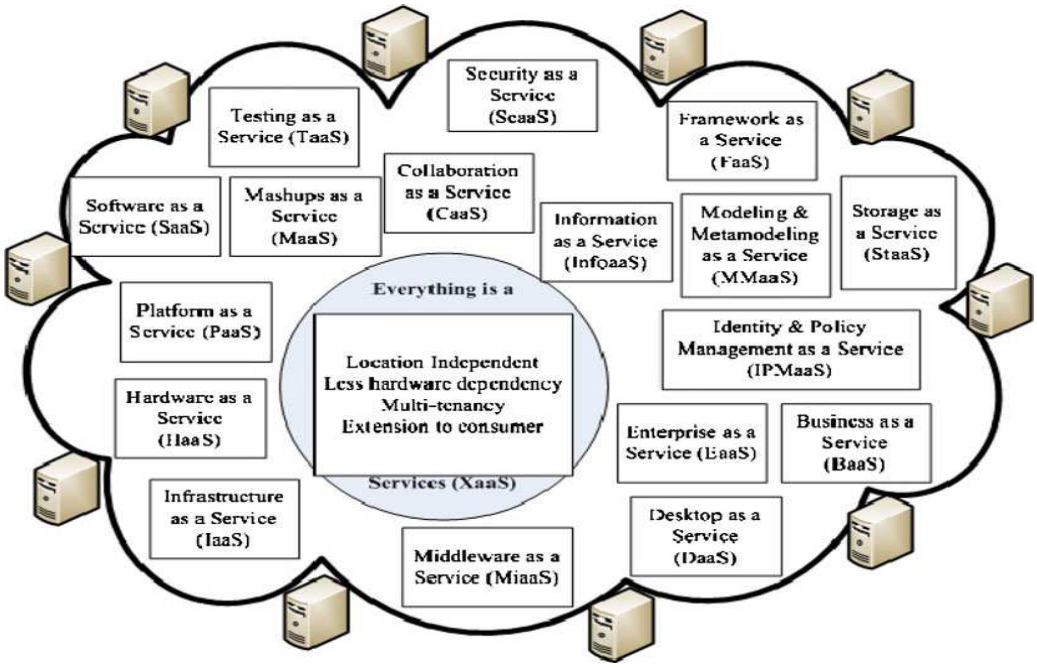
2. Services that provide functionality for cloud computing environments (such as special billing software that ensures that cloud computing environments of different sizes and with different levels of service can be provided by the service charge)

3. Consulting services that help organizations transform and transition to cloud computing

4. Application services provided in cloud computing environments that offer application developers a standardized application functions (eg routines for authentication, search, the implementation of policies or processes according to ITIL)

Rimal et all [5] shows that the cloud can be seen as super services, i.e., providing "everything" as a service. Also shows that the concept of the cloud as a service is not new, but it is an evolutionary development of various previous initiatives, which at the time of its creation, ahead of development. Recall that here, renting computer time has been known since the inception of computers, systems, client - server are also long known, virtualization was already possible in the time of mainframes, etc.

Fig. 1: Cloud as a service "everything"according to [5]

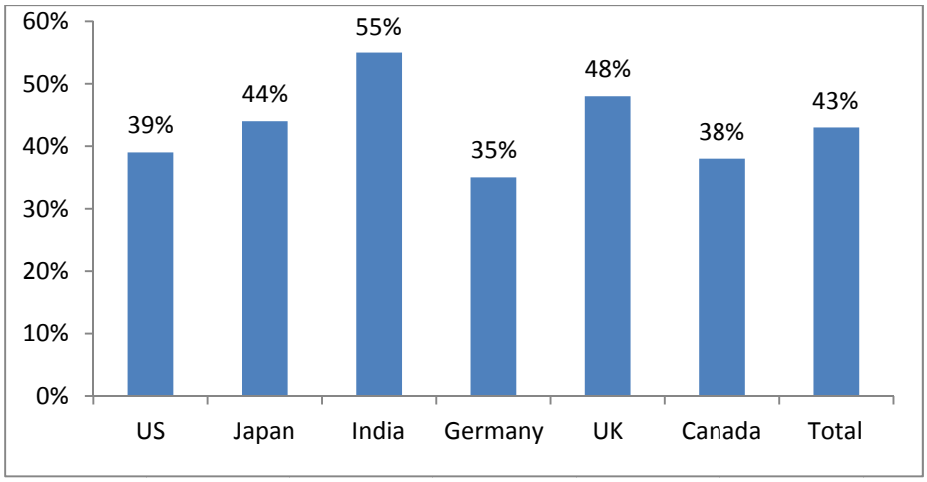


Source: [5]

4 Information security in the Cloud

According to a recent global survey (conducted in May 2011) between 1200 responsible persons from the USA, Great Britain, Germany, India, Canada and Japan (from companies with more than 500 of employees) conducted by Trend Micro [7], was revealed uncertainty and concerns about their journey to the cloud. In this global survey almost half (43%) of those persons responsible for making decisions on corporate IT in the past 12 months, on the side of the cloud vendors, recorded errors or problems in securing the cloud.

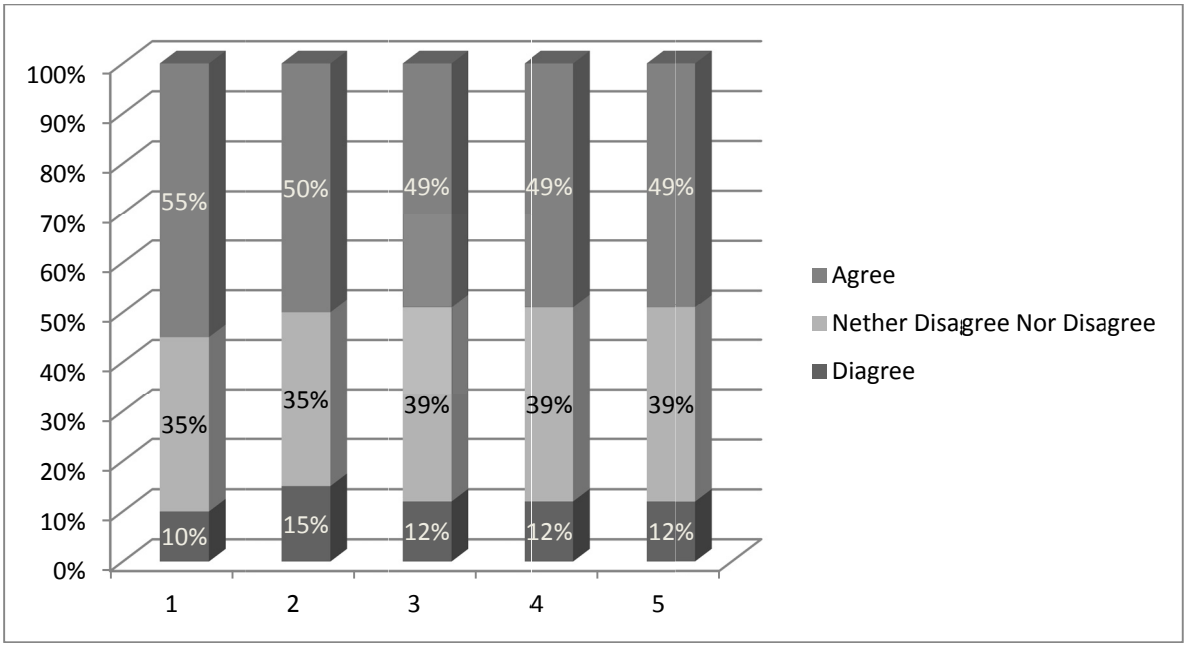
Fig. 2: Safety evaluation of the cloud according to [7].



Source: [7]

Another interesting question from Trend Micro [7], Questionnaire
Q: How much do you agree or disagree with the following statements about cloud vendors / cloud computing services?

Fig. 3: Statements of the cloud vendors / cloud computing services according to [7]



Source: [7]

Where denoting of X- axes meaning:

1 – Shared storage is vulnerable without encryption.
2 - Apprehension over security is a key reason holding back our adaption of cloud technologies.
3 – A guaranteed SLA would drive us to use more cloud computing services/cloud vendors.
4 – If knew more about how to secure our data in the cloud, this would increase our consideration of using the cloud.

5 – An easy to administer cloud encryption service would give us reason to consider using more cloud services/cloud vendors.

Conclusions of previous investigations are not surprising. In the cloud are no longer traditional boundaries between what is inside the company, and what is outside. Many services now operating within the institution is moved (outsourced) to other operators and a growing part of business processes to take place on the Internet. And it is well known that from the perspective of security much more complicated than the internal corporate network.

Although the storage information stored encrypted, so you must be decrypted before processing, because in an encrypted form cannot be further processed, it can be a source of leakage. Another reason for this is that the service provider cannot beneficiaries of services to provide physical control over the data that you stored in the storage cloud.

Conclusion

The article discussed the currently very topical issue of information security related to cloud computing, which is in service at the forefront of professional interest of the community. In terms of information security not yet all has been resolved. Even when there has been a non-profit organization estabilished. Cloud Security Alliance (CSA) [8], which seeks to introduce cloud computing universally binding standards which providers would have to follow, the results are still small. CSA is made up of manufacturers of security solutions, independent experts and providers of cloud services.

Ackowledgement

This article was supported by grant provided by the Ministry of Interior No. VF20112015018 "Bezpečnost občanů – Krizový management"

References

[1] Cloud [cit. 2011-09-15]. Available at WWW: <http://www.cloud.cz/cloud-computing/158-cloud- computingco-ty-pojmy-znamenaji.html>

[2] KOSTIHA, F. *Bezpečnost informací. Ikaros* [online]. 2006, roč. 10, č. 5 [cit. 2011-09-28]. Available at WWW: <http://www.ikaros.cz/node/3332>. URN-NBN:cz-ik3332. ISSN 1212-5075

[3] POŽÁR, J. *Vybrané hrozby informační bezpečnosti organizace*, [cit. 2011-09-28]. Available at WWW: <http://www.cybersecurity.cz/data/Pozar2.pdf>

[4] PŘIBYL, T. *Outsourcing bezpečnosti: nemilovaný, leč nutný* [cit. 2011-09-28]. Available at WWW: <http://www.ictsecurity.cz/odborne-lanky/outsourcing-bezpenosti-nemilovany-le-nutny.html>

[5] RIMAL, B., JUKAN, A., KASTROS, D., GOELEVEN, Y. *Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach. Journal of Grid Computing* Volume 9 No 1/ 2011 pp 3-26 ISSN1570-7873 (Print) 1572-9184 (Online)

[6] ŠVEC, P. *Cloud computingu v praxi: cloud a bezpečnost* [cit. 2011-09 15]. Available at WWW <http://www.itbiz.cz/cloud-computing-v-praxi-cloud-a-bezpecnost-1>

[7] http://www.cleverandsmart.cz/cloud-computing-bezpecnost-v-cloudu-a-rizika/

[8] Cloud Security Alliance (CSA) – security best practices for cloud computing. (2009).Retrieved April 16, 2012, from <http://www.cloudsecurityalliance.org/>

[9] BERRE, A. J., ROMAN, D., LANDRE et al. (2009). *Towards best practices in designing for the cloud. In Proceeding of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications* (pp. 697-698). Orlando, Florida, USA: ACM. Retrieved from <http://portal.acm.org.library.capella.edu/citation.cfm?id=1639950.1639970 &coll=portal&dl=ACM&CFID=80867670&CFTOKEN=24312614>

[10] HAYES, B. *Cloud computing. Commun. ACM*, *51*(7), 9-11. Retrieved from <http://portal.acm.org.library.capella.edu/ft_gateway.cfm?id=1364786&type=html&coll=portal&dl=ACM&CFID=80867670&CFTOKEN=24312614>

[11] CloudStandards. (2010). Retrieved April 16, 2012, from <http://cloud-standards.org/wiki/>

[12] OWASP. (2010). Retrieved April 16, 2012, from <http://www.owasp.org/index.php/>

[13] JÄÄTMAA, J. *Financial Aspects of Cloud Computing Business Models*. 2010 Retrieved April 16, 2012, from <http://www.intertic.org/Policy%20Papers/Jaatmaa.pdf. >

[14] ARNHEIM, D. *Top Four Cloud Computing Models. Available at www:* <http://cloudcomputing.sys-con.com/node/1546627>

[15] ARMBRUST, M., FOX, A., at all (2009) *Above the Clouds: A Berkeley View of Cloud Computing,* Retrieved, April 16, 2012 from <http://radlab.cs.berkeley.edu/>

Contact Address

prof. Ing. Jan Čapek, CSc.
University of Pardubice, Faculty of Economics and Administration, Institute of System Engineering and Informatics
Studentská 94, 532 10 Pardubice, Czech Republic
e-mail: capek@upce.cz
Phone: +420466036511

Received: 01. 05. 2012
Reviewed: 30. 06. 2012
Approved for publication: 01. 11. 2012