Sustainable Cloud Computing

DOI 10.1007/s12599-011-0159-3

The Authors

Prof. Dr. Günter Müller (✉)
Department of Telematics
Institute for Computer Sciences
and Social Studies (IIG)
University of Freiburg
Friedrichstr. 50
79098 Freiburg
Germany
mueller@iig.uni-freiburg.de

Prof. Dr. Noboru Sonehara
Prof. Dr. Isao Echizen
Dr. Sven Wohlgemuth
National Institute of Informatics (NII)
2-1-2 Hitotsubashi, Chiyoda-ku
Tokyo 101-8430
Japan
Sonehara@nii.ac.jp
iechizen@nii.ac.jp
wohlgemuth@nii.ac.jp

Published online: 2011-04-15

This article is also available in German in print and via http://www.wirtschaftsinformatik.de: Müller G, Sonehara N, Echizen I, Wohlgemuth S (2011) Nachhaltiges Computing in Clouds. WIRTSCHAFTSINFORMATIK. doi: 10.1007/s11576-011-0273-3.

Cloud Computing is today's most promising technology due to its cost-efficiency, flexibility, and lastly its vision of unlimited and unrestricted access to computing for everybody. It is this expectation of an easy to use and affordable world of services that has already given Cloud so much attention. For instance, smart-phones give access to the Cloud and have replaced traditional mobile phones. While private users are ready to accept the new services, there is resistance in business. Despite a surge in interest, activities, and investments, there are reasonable scenarios that may eventually compromise the globally shared hope of Cloud as a new IT procurement paradigm. Still today it is unclear which application areas of IT can and will be outsourced to a Cloud. The hesitation is mostly over the concerns about loss of control over critical company data and of relationships with customers. A surprising and less discussed aspect of the sustainability of Cloud Computing has emerged in Japan, where the IT-Cloud infrastructure is primarily conceived as a means to support resilience in cases of natural disasters, and is only provided secondarily for public and industrial use.

Sustainability has become a marketing buzzword in IT, for anything relating to the reduction of ecological key indicators. From this point of view, sustainability is a synonym for modernity promising an improved input-output relationship on a global level. IT offers at least two types of sustainability. The work on "Green IT" considers computers as part of the problem due to their intensive energy consumption; e.g., for operation and cooling. This is the case for the Cloud clusters, which is still a hidden, but nevertheless existing ecological issue for society. "Green IS", however, considers computers as part of the solution due to their capability to replace the current "develop and destroy" mode of production by a more regenerative or nature-preserving mode. The present claim of "Green IS" is that Cloud offers services and realizes scale effects that the IT of today, neither in a company nor by a specialized service provider, can ever accomplish. Benchmarking and standardized processes enhance the level of any business due to the fact that computing services can be acquired on demand.

However, there is a third aspect to sustainability that deals with the loss of control by individuals as well as businesses and governments. Quality criteria such as security and privacy, especially the protection by a legal landscape of a country, avoidance of unwanted information flow, and of data misuse define the risk- level any service requester encounters when delegating data and services to a Cloud. In this special focus issue of BISE, but also in the scientific discourse worldwide, this third aspect is considered to be the dividing line between sustainable and non-sustainable Cloud Computing. Any system is considered not sustainable if it cannot protect data or assure a required computing quality. With their required availability and flexibility for disaster management, the Japanese case demonstrates a new, rarely discussed property of sustainability.

At present, the industry most fit and equipped to exploit the benefits of Cloud Computing, has a very hesitant attitude with regard to using Cloud innovations inhouse. According to Merill Lynch (Chow et al. 2009) only the software company "Salesforce.com" operates on a Cloud, while the top five software companies (ranked by sales revenue) have only selected Cloud offerings. The reason for this is that they shy away from outsourcing their sensitive data into an environment, which they do not consider reliable and controllable. Those who have joined the Cloud already only outsource their less sensitive data, while complex processes and sensitive data remain in the company's premises. It remains a paradox, however, that contrary to the original Cloud vision where the user should not worry where the computing physically takes place, the anonymity of the computing location has actually been the one key factor limiting the growth of Cloud Computing. This lack of trust is explained by technical principles, which in Clouds are identical to social networks, like Google or Facebook. Technically, any delegation of computing enables the service provider to carry out the analysis of customer's data, collection and transfer of private data and data mining for inferences, and the set up of profiles on the performance of customer's business models. Because of this lack of control, most of the larger stock market registered companies are careful not to make steps towards the Cloud too fast. This fear also extends towards controlling the behavior of employees in their use of social networks and even e-mail and the web. The reason may sometimes be a moral one, when employees merge leisure and work objectives, but mostly, it is also the fear of espionage and sabotage. The technology driven *smarter planet* initiative by IBM,[1] and the program *Internet of Services* in Europe[2] depend upon moving Cloud Computing from vision to reality. Acceptance in business will depend upon transparency of data handling, process execution, and information flow to improve trust of customers in the Cloud processes. Still today there is a lack of useful and applicable mechanisms to ensure transparency with regard to loss of control. The Japanese strategy for Cloud Computing puts the objective on the improvement of existing social infrastructures, called the five E's, i.e. steady supply of (1) energy, improving (2) education and new (3) employment opportunities, as well as preserving the (4) environment, and to ensure a participative life of the (5) elderly. Aoyama et al. describe the use of Inter-Cloud Computing for disaster management. Inter-Cloud Computing is just one of many projects that makes the Japanese Cloud strategy become reality (Government of Japan 2011). Their understanding of sustainability point to the fact that loss of control may not be the only security property to be followed, but needs to be complemented by redundancy to ensure availability and flexibility. In the interview in this issue, Watanabe stresses that sustainability, when understood in this extended sense, is one of the guiding principles for Japanese Cloud strategy.

When designing or evaluating sustainability of solutions for these requirements in Cloud Computing, it is helpful to realize that many of the issues are "old wine in new barrels", although they may be more pressing now due to economic arguments with regard to lowering the IT costs. Given the overcapacity of today's computing power coupled with the possibility to interconnect, prices for computing fall to a very low level, while IS-development costs remain high. Also here, Cloud Computing offers a solution which is called service on demand. Services also have the danger of loss of control, because no user can be sure yet that the service does what the service claims to do. With regard to sustainability it is the issue of use of data and quality of service. For problems like this, it helps to recall the situation when the IT industry was faced with the advent of open source software. Transparency of open source software was then a positive argument to differentiate the services of open source compared to proprietary offerings. The cost argument along with the international standardization enabled IT departments or start-ups to quickly build and employ new applications, and finally assured the breakthrough of open software. The check of correctness of open source programs was delegated to trusted parties or evaluations have to be drawn from public use; e.g., by collaborative filtering, and last but not least the source code was public. The latest examples of the impact of the public and their surveillance are the vulnerabilities of many web services. However, the similarities of these "old" problems and the new Cloud issues are a reason for optimism that the "new" Cloud problems may be solvable, since they have had at least foundations for solutions for quite some time.

For example, consider the present understanding of privacy and security. The theoretical limit in security and privacy is that if the network and adversarial model are not fully defined, then all "secure" protocols can be broken. If the adversary is unknown, then security becomes unsolvable, since it is not clear what is and what is not protected against. How do we know what is relevant to security before an attack even happens? Are the threats identical to actual attacks? All security mechanisms are designed around the "ideal" model paradigm, where all involved parties are defined ahead of action and they only send inputs to trusted parties, who compute the task – without any own interest – and send the outputs back. Cooperative Services, as e.g. offered by Google and Facebook, demonstrate that between "ideal" and "real" there is a deficit not only challenged by hackers, but also a source of income by respected companies. In Cloud Computing both providers and clients are faced more than ever with a "real" security and privacy model. Cloud networks are dynamic and not set up for a closed user group. Sonehara, Echizen, and Wohlgemuth make an interesting proposal to treat service isolation in a Cloud with classical privacy mechanisms. As a first step, they request to define security policies as the reference for a convergence of the ideal and the real model. The second step is to ensure the correct usage of the service and to control and report unwanted flow of information. Mechanisms for this include the delegation of rights, whose realization is supported by a secure protocol between user and provider.

[1] http://www.ibm.com/smarterplanet/us/en/.

[2] http://ec.europa.eu/information_society.

Accorsi, Lowis, and Sato suggest an audit-oriented approach to overcome the theoretical security deficit. The principle is that "after" execution of a service by exploiting secure logs of the transaction, the "real" security model can be reconstructed and compared to the "ideal" model. This comparison identifies attack patterns, which help to increase knowledge of threats "before" execution at design time. These patterns are the inputs to issuing certificates serving as documents to express sustainability guarantees by a third party. While attacks may not be prevented, the consequences are detected and can be traced back to the reason of vulnerability. The paper by Kerschbaum deals with the issue of how much information is to be conveyed, if a set of parties cooperate. The work is based upon the fundamental theory of computational indistinguishability, which was proposed by Yao in 1987. The assumption is that honest parties adhere to security protocols and produce their output as instructed. Authenticated channels can already be achieved now using a public-key infrastructure of digital signatures. For any "Quality"-Cloud provider the challenge is to allow a client to query a database without the Cloud server learning what the query is. The proof for trustworthiness is the guarantee that an honest client obtains a correct result. Isolation will be maintained or detected even if a malicious server is used. Kerschbaum gives a possible solution to isolation of clients and ensures privacy against unwanted information flow. His criteria are that the client's query A is indistinguishable from the Clouds view when the client's query is B.

This special issue of BISE has a terrible actuality because of the catastrophes the people of Japan are enduring at this time. Besides efficient reconstruction, many victims will have to struggle for a long time to get back to a normal life. They also need help from us. We would like to thank all, who have helped.

References

Chow R, Golle P, Jakobsson M, Shi E, Staddon J, Masuoka R, Molina J (2009) Controlling data in the cloud: outsourcing computation without outsourcing control. In: Proceedings of the 2009 ACM workshop on cloud computing security, CCSW'09, pp 85–90

Government of Japan (2011) Highlighting Japan, vol 4, February 2011. The cabinet office. http://www.gov-online.go.jp/eng/publicity/book/hlj/