Security and Privacy Implications of Cloud Computing - Lost in the Cloud

Vassilka Tchifilionova

National Laboratory of Computer Virology,
Bulgarian Academy of Sciences
1113 Sofia, Bulgaria

Abstract. Cloud computing - the new paradigm, the future for IT consumer utility, the economy of scale approach, the illusion of un infinite resources availability, yet the debate over security and privacy issues is still undergoing and a common policy framework is missing. Research confirms that users are concern when presented with scenarios in which companies may put their data to uses of which they may not be aware. Therefore, privacy and security should be considered at every stage of a system design whereas advantages and disadvantages should be rated and compared to internal and external factors once a company or a person decides to go into the business of cloud computing or become just an user.

Key words: Cloud computing, privacy, data, network, security, information.

"As long as we live and breathe we'll be paranoid. We always have to be careful, but it isn't going to stop the movement of this technology" (David Barram)

1 Introduction

The need to search and meet ever increasing IT demands has often been seen and based on purely an economical base, transforming computing into a utility where performance and efficiency have become a part of the product. Internet was just the tool, the infrastructure that provided the platform for utilization of new services.

Cloud computing has already proved that it can reduce infrastructure costs and offer the ability to pay for services only when requested. Some experts even argue that services delivered via cloud computing should be used as a public utility [1].

In a similar way, others argued that companies will increasingly purchase IT as a utility service from outside suppliers [2]. Others call it the "age of planetary computing" [3].

The cloud computing has been on the market for years (e.g. Microsoft Exchange/SharePoint, Google Apps, Amazon's Simple Storage Service, Twitter, Facebook and others) but it was analysed in details by professionals the last two years ago and it took some time until a common definition emerged. One of the very recent working definitions is brought up by the United States National Standards for Information Technology that defines cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [4].

Cloud computing is based on abstraction of infrastructure, it is service oriented with the opportunity to offer dynamics and elasticity and at the same time minimise consumption and billing. The abstraction level takes part between the physical infrastructure and the owner of the information being stored and processed. The most common model of cloud computing consists of the three major components: software, platform and infrastructure.

Consumers are not paying for infrastructure, rather they pay for capability. For instance, Microsoft's product Exchange and SharePoint are available online for a monthly subscription instead of buying the full license for their use. This provides for a better utilization of computing resources. In addition, it has also an application in the national security domain which allows the intelligence community to execute missions at all levels by utilizing simultaneously the large volume of capabilities the technology can offer [5].

To understand the scale of cloud computing, one should look at analysis that estimate that within the next five years, the global market will grow to 95 billion dollars and that 12% of the worldwide software will move to the cloud [6]. Another study reveals that 66% of Americans connected to the Web use some kind of cloud service since most popular consumer-facing services that enable better collaboration are cloud based [7].

The most important question a company or a natural person should ask itself is not whether to move to a cloud but what part of the IT to move. Researchers argue that companies are forced to switch over to cloud computing in order to meet business' needs. Given the dynamic business environment and the focus on globalization, there are only a few enterprises that do not outsource some part of their business [8].

One can argue that this new approach is the future of networks capabilities and an innovative economical tool that would help companies to boost their performance by outsourcing fully their information systems and information technologies. But there are hidden costs and these are reputation, security and privacy. There are even experts that argue that the definition of cloud computing is unclear and that the benefits to the business are not being presented well [9]. The objective of this paper is to give the essence of security and privacy concerns that this new technological mean is facing and thus be a virtual

checklist for all managers who consider or have considered the implementation of could computing approach. We are reaching a point where the implementation of cloud computing is inevitable.

2 Security Implications

It is well accepted in the business world that along with the benefits come risks and security concerns that must be taken into account. Managers should also consider the fact that new initiatives are most likely, unless fully examined, to bring potential for high risks. In general terms, information security is often associated with the tree principles of confidentiality, integrity and availability. Security risks such as viruses, Trojans, warms, spoofing, root kits and many others should not be ignored. Once they get into the cloud not only a single "customer" is at risk but the whole cloud with all its users. In that sense the security implication of a weak IDS and IPS will only increase the scale of damages caused not only to the cloud owner but to all the parties involved.

The very most well defined security concern is the abstraction between the physical infrastructure and the owner of the information being stored and processed. The traditional approach is based on the ownership of computer hardware where the data is stored. With cloud computing consumers do not own the computing infrastructure and often it is no longer clear who owns and controls the data if the third party is further outsourcing some of its infrastructure or services [10], [11] or if the real owner is not mentioned in the provider's term of services. For example, if a government agency owns the provider, terms of service that allows sharing with affiliates could result in all of the user's information being obtained by prosecutor or intelligence agencies without further notice or process. In most cases, the provider would also maintain a full record of user's activities and these records for instance might be well used in a law case [12].

There is always the risk of compromising confidential information by third parties. Users are required in most cases to establish their identity by providing personal information [13]. With regard to this, personal information could be misused if not properly protected. The cloud provider has also responsibility to safeguard this personal information in accordance with the data protection legislations.

In general, critics do not accept counter-arguments that cloud computing may reduce the number of severity of breaches in comparison to those suffered by desktop users, as well as users who store data with third parties outside the cloud [14].

Criticality of the data handled is yet another risk to be considered. Security is no longer of use if the data is not stored and managed in a proper way. The cloud is a very dynamic structure and in time of crises and disasters information can not be available not to exclude also the unavailability of Internet at the user's end because of his physical location. That is why an important part of any contract should be the incident response policy. It is unrealistic to expect that no incident will ever happen with a cloud service provider irrespective of

the measures he has taken to restrict damages and impact. This can also be linked to the physical risk which is also a major security concern. The facility where the data is stored should have adequate measures for physical protection.

The level of risk can be determined by whether an organization is outsourcing a service or infrastructure or not. In that sense, in a multi-tier service provider arrangement, each of the parties involved share the risk of security.

Companies providing cloud services need to understand that authorisation is a key point when dealing with many customers. Methods such as two-factor authentication are desirable but it is a question of applicability. If a company uses this method it has to reflect on whether it is possible to transfer it to the cloud and what the implications would be?

Current cloud computing security is weakened by the fact that most companies don't have a cloud strategy yet [15] and those who have, very often, over time not update their security policies and it is quite possible that they do not meet the current threats and vulnerabilities which make the security procedure very "relaxed".

Users should be well aware of what they can and cannot do in the cloud and therefore it is critical to set up their rights and responsibilities at the very start. Yet another problem is again whether the cloud provider would support a role-based model which will allow users to know exactly their user rights and to access that particular data or service for which they are authorized to.

Many cloud providers use third-parties for security audit and so they show their willingness to be accountable and reliable to their customers. The audit itself could be followed by obtaining some form of an accreditation. In general there are two benefits of an audit report: it evaluates the security risks of the cloud provider and so it gives a feedback to the user and on the other hand, it is beneficial to the cloud provider for future improvements.

However, there are certain systems which are not subject to audit by external auditors since the legal regulations do not allow such. Such an example is the US Health Insurance Portability and accountability Act [16], [17].

There are different clouds with different security models and it is up to the manager to assess the services he would like to outsource or take advantage of and the residual risks that would be the result of his choice. The human factor should not be excluded [18]; it is indeed one of the highest security risks in any company. The people who are "running" the cloud should undergo a background check otherwise a company may face not only theft of data but also lack of competence in running a cloud service.

Once the expectation of the parties involved are clear, one can set up clear rules with regard to handling, use, storage and availability of information. A solution to the security problem would be the proper classification and labeling of information.

In addition to the above mentioned risk, there is also the possibility that the cloud provider may behave unfaithfully with regard to the users' outsourced data. For instance, for monetary reasons, reclaiming storage by discarding data

that has been rarely accessed or not accessed at all, or in the worst case, hiding data loss as to maintain a reputation [16].

The common practice of cloud providers to encrypt data does not imply that clients should not encrypt data themselves before sending it [19]. However, if an intruder can figure out how to access your information in the cloud bypassing all authentication means he potentially can access all data and services.
Cloud services should be addressed clearly by information security policies of the companies.

A recent survey by ENISA indicates the most important risks: lock-in, failures in mechanisms separating customers' data and applications, and legal data protection legislation [20].

Many experts argue that unless one's company is in the security business it is quite clear that one's company would be less secure [13]. With that respect, cloud providers should use the principle of applying the highest security measures to the most risky client that would be in the cloud. Although security can be the weakest link of many cloud providers it can be also the strongest advantage of a service provider whose core business is information security. Therefore, one can argue that when we compare internal versus external information security we can be in favor of external.

Some cloud computing service providers argue that cloud computing is more secure than desktop-based and enterprise computing [3]. If the right security measures are in place on can argue that no data can ever be lost when a laptop is stolen or a desktop is attacked by unauthorized users since data is kept on private clouds and encrypted with access only provided to authorized users [2].

The reason for that is very simple: Many companies have IT security as their core business. In order to examine why IT security is hard to achieve we should consider the following [21]:

1. The number of highly skilled and experienced security technologists is very small.
2. Good security is expensive.
3. Your IT and security staff has an interest in the contents of your data.
4. Any resource (employees, contractors, service workers) in your organization that has access to your datacenter has access to all your data.
5. Most internal IT organizations grew with the business (Meaning that different systems over the time share common infrastructure).

And what happens if a vendor goes out of business?

To sum up, one of the few very important security issues before selecting a cloud vendor should cover privileged user access in order to know what people are oversighting such information and what the control over their access is. At second place, vendors should be willing to undergo an external audit and authentication. And last but not least, a vendor should state where exactly data is stored, under which jurisdiction and whether they will make a contractual commitment to obey privacy requirements [22].

3 Privacy Concerns

In the context of European data protection the issue of data security is very much bound to the data controller who is responsible and remains such for the collection and processing of personal data also in the cases where data is processed by a third party. Some European data protection authorities require data controllers to obtain a prior consent before data is transferred abroad and very often this is followed by a detailed description of why this needed and the means for protection of the receiving body [23].

It has to be stressed that not all types of could computing raise the same privacy and confidentiality risks. It is depends what type of information is published and the way it relates to a particular person and whether it was published with his consent. In reality these rights are ignored since consent has become a mechanism for guaranteeing continuous data flows, rather than a tool to protect individual rights [24].

The most common form of explicit consent nowadays is still the written contract. However, in the world of electronic transactions explicit consent is not that easy to come by. There is no comprehensive protective framework for safeguarding interests in the face of privacy of these new emerging technological applications.

Virtually every government worldwide would have a regulation that would allow an access to information that resides on a cloud. Cloud providers should discuss all these privacy and security implications and if necessary encrypt the data. This should be done in accordance to the current governmental legislation as not to be later considered a national threat.

A clear example for what the Government can do is the Patriot Act in the United States [25] where the federal government has the right to request details of ones online activities without the knowledge of the person. With that respect sometimes the forensics procedure may not be clear and so a third party can access your information in the cloud.

On the other hand, although the Government may have his legal right, a bigger concern should be the weak security systems of the websites where a phishing attack or key logging can happen easily. Even more than before, the importance of a strong password and any other form of authentication has came up so important [26].

It is quite interesting to note that information could be physically located in two or more different locations. And if the vendor moves this information without the knowledge of the owner then it is the case of changing the legislation and therefore suffering different legal consequences.

The trend toward adopting privacy and data protection legislation has continued consistently to the present. Most central European nations, as well as other jurisdictions, such as Australia, New Zealand and Hong Kong, now have so called "omnibus" data protection legislation.

The United States, however, has not adopted omnibus data protection legislation. The current culmination of three decades of European policy development

is reflected in the European Directive 95/46/EC [27]on the Protection of Individuals with the Regard to Processing of Personal Data and on the free Movement of such Data.

The EU Directive contains a significant extraterritorial provision that the flow of personal data from any EU member country may be halted, if the jurisdiction to which it is being transferred is deemed not to have an adequate level of protection for personal data. American companies doing business in Europe have had to adhere to the data protection laws of each of the jurisdictions in which they operate. As a matter of fact, many American companies know how to and have been complying with omnibus data protection legislation in the countries that require it. The irony is that these companies may not be providing the same level of protection of personal data for Americans or individuals in other parts of the world where there is no statutory requirement. Law seems to be powerless when it comes to international boundaries [28].

There is a common practice of cloud service providers to keep information in place after it has been removed from the user is in place. Most social networks misuse the information of their users and do not inform them about the privacy changes they made and in the worst case they inform them after the actual change leaving the users with no choice to delete or edit the information they have uploaded on the cloud.

In many instances a user may not be aware of the existence of a second-degree provider and often the cloud provider offers its facilities to the users without an individual concept. Changing the terms of the policy without limit would find a user a step back when he realizes that the privacy policy has changed and he has not had the opportunity to remove sensible data.

One of the greatest privacy concerns is the risk of compromise of confidential information which can pose a significant complication with regard to the fact that data could be handled and stored in different geographical locations. Compliance to regulations and laws in different geographical locations can be quite challenging. Although the legislation itself could be a solution to the privacy problem, during the years it has proved that in certain cases it would fail [23] Unless there is a legislation explicitly governing cloud computing, no security means would be able to substitute for it. It is often the case that law is behind the technology developments.

Another security risk posed by could computing is the mix up of information assets which is usually the result of high-availability systems without the set up of private networks [7].

In March 2009 the Electronic privacy information center filed a complaint and request for injunction before the Federal trade Commission exposing the security flaws of Google's Cloud Computing. In the above mentioned case, Google was unable to protect usernames and passwords allowing outsiders to "snoop on users' e-mail", another vulnerability was the security flow resulting from a vulnerability in Google desktop and Internet Explorer. [29].

Privacy is not only about companies' and enterprises' data but it is very often a matter of revealing personal information as it was in the case of Google.

A more recent case was brought up to the light in February 2010 when the an Italian judge decided to invoke a six-month suspended jail sentence on Google's global privacy council and two other company executives. This case proves the public need to maintain privacy and to make even executives accountable which is also believed to be the first time in privacy history [30].

Users should be enabled to give informed consent once the cloud provider proves that they are trustworthy and handle the information with care. The privacy commissioner of Ontario argues that companies need to understand that identity management is not only a business process but also a user activity. The infrastructure must account for many devices and allow for a unified user experience over all devices [31].

It is common for a cloud provider to offer cloud services or infrastructure without individual contracts. If the user is bound by the general published terms of services it would be very difficult to stop the provider to acquire a variety of rights on the information [12].

It could also happen that the cloud provider acquires information that reveals transactions and relations which may have purely a commercial value. The simplest example would two companies negotiating a merger or being rivals on the market.

The core of privacy that law protects should be clearly defined in terms of harmful uses and remedies. Imaginary harms must be addressed by communication and education, not by legislation and regulation [32], [33] Once people understand the business use of information, the benefits of free flow, and the cost of privacy, their privacy preferences may well appear to be not what we believe them to be. One of the latest developments in this area is the launch of the Privacy Impact Assessment by the UK Information Commissioners Office [34]. Similar Acts exist also in the USA, Canada and Australia where privacy commissioners are the primary privacy and data protection authorities. Most commonly, concerns arise when it is not clear why their personal information is requested or how it will be passed on to other parties [35].

4 Conclusions

Companies need to be very specific in choosing a provider. Accountability is one possible way to state the responsibility of the company offering cloud computing services independent of the place it resides or is processed. Still, legislation should be in place and must be a must.

There is no doubt that cloud computing is becoming more of a utility than simple capability delivered over a network. One big advantage is the concept of risk-share but if you do not know what you are sharing then you can not define and demand a proper security frame. Furthermore, only the minimum information should be collected or stores, and so inform the users what type of information one is storing and for what purposes.

Unless your organization in the security business it is likely that the company will be less secure than the cloud provider. For that reason, one should first

compare the levels of security of his company and the cloud provider. Cloud computing has significant implications for the privacy and security of information not only for private but also for business information.

Security and privacy will remain a major concern until users become fully aware of the "depth" of the cloud: who manages it, how he does it and whether the company can afford to "give away" its information - decision that can only be taken after a careful risks analysis and policy considerations otherwise we may simply get lost in the cloud.

References

1. Mohamed, A. A history of cloud computing. `www.computerweekly.com`, (2009)
2. Gourley, B. Cloud Computing and Cyber Defense. A White Paper provided to the National Security Council and Homeland Security Council as input to the White House Review of Communications and Information Infrastructure, Crucial Point LLC, (2009)
3. Reingold, B., Mrazik, R. Cloud computing: the intersection of massive scalability, data security and privacy (Part I). Cyberspace Lawyer, [FNa1] 14 No. 5 GLCY-LAW 1 Page 1 14 NO. 5, Cyberspace Law. 1, LegalWorks (2009)
4. United States National Standards for Information Technology, http://www.nist.gov/index.html
5. Dataline White Paper: Cloud computing for national security applications, http://www.dataline.com/soar.htm
6. Merrill Lynch, www.ml.com
7. Bruening, P., Treacy, B.:The Bureau of National Affairs, Inc. Cloud Computing: Privacy, Security Challenges , Privacy&Security Law. PVLR ISSN 1538-3423, (2009)
8. ISACA. Emerging Technology. White Paper Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives (2009)
9. Flinders, K. Microsoft slashes cost of cloud computing, www.computerweekly.com (2009)
10. Webbmedia Group's Knowledge Basem, Cloud Computing Explained http://www.webbmediagroup.com (2009)
11. Binning D. Top five cloud computing security issues, www.computerweekly.com (2009)
12. Gellman, R. Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, World Privacy Forum (2009)
13. Bertino, E., Paci, F., Ferrini,R., Shang, N. Privacy-preserving Digital Identity Management for Cloud Computing, CS Department, Purdue University Bulletin of the IEEE Computer Society Technical Committee on Data Engineering
14. Reingold, B., Mrazik, R. Cloud computing: Industry and government development (Part II).
15. Zimski, P. Cloud computing faces security storm www.computerweekly.com (2009)
16. Wang,C., Wang,Q., Ren,K., Lou, W. Privacy-Preserving Public Auditing for Data Storage: Security in Cloud Computing, Illinois Institute of Technology, Chicago IL 60616, USA, Worcester Polytechnic Institute, Worcester MA 01609, USA (2009)
17. 104th Congress, The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191), http://www.cms.hhs.gov/hipaageninfo/downloads/hipaalaw.pdf

18. Yee,A. Cloud Computing Security Risks - Are they real?, www.ebizq.net (2009)
19. Andrei, T. Cloud Computing Challenges and Related Security Issues, p.5 (2009)
20. ENISA: Cloud Computing Benefits, risks and recommendations for information security , Report (2009)
21. Almond, C.: A Practical Guide to Cloud Computing Security: What you need to know now about your business and cloud security, Avande (2009) www.computerweekly.com (2009)
22. Brodkin,J.: Gartner: Seven cloud-computing security risks, Network World, www.infoworld.com (2009) www.computerweekly.com (2009)
23. Tchifilionova, V.: "The mirage of law - an oasis for surveillance' (in Bulgarian/English) , International politics, vol.4, p.7-23, ISSN 1312-5435, South-west University "Neofit Rilski" Press, Blagoevgrad, www.computerweekly.com (2009)
24. Davies, S.: "Unprincipled privacy: why the foundations of data protection are failing us", University of New South Wales Law Journal, http://www/austlii.edu.au/au/journals/UNSWLJ/2001/7.html (2001)
25. 107th Congress, The Patriot Act, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf (2001)
26. Trapani,G: The Hidden Risks of Cloud Computing, Lifehacker (2009)
27. 95/46/EC Directive of the European Parliament and the Council, http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf (1995)
28. Hurley, D.: "A whole world in a glance: privacy as a key enabler of individual participation in democratic governance", Harvard Infrastructure Project, Harvard, http://www.pco.org.hk/english/infocentre/conference.html (2001)
29. EPIC, Before the Federal Trade Commission, Complaint and request for Injunction, In the Matter of Google, Inc. and Cloud Computing Services
30. Vijayan, V.: Google privacy convictions in Italy spark outrage, www.itworld.com (2010)
31. Cavoukian, A.: Privacy in the clouds: A White Paper on Privacy and Digital Identity: Implications for the Internet, Information and privacy commissioner of Ontario (2009)
32. Bergkamp,L. et al: "EU Data Protection Policy", Computer Law and Security Report, Vol. 18/1,2002 (2002)
33. Litan, R. : "Balancing Costs and Benefits of New Privacy Mandates", AEI-Brookings Joint Canter for Regulatory Studies, working paper 99-3, April 1999, (1999)
34. The Information Commissioner's Office, PIA's Book 2007, http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html
35. Pearson, S.: Taking Account of Privacy when Designing Cloud Computing Services. HP Laboratories, HPL-2009-54 (2009)