Source: **Marko Hölbl** **Version** **V17/15.03.2011**

Document for:

Decision	
Discussion	
Information	X

Cloud Computing Security and Privacy Issues

CEPIS

The Council of European Professional Informatics Societies (CEPIS) is a non-profit organisation seeking to improve and promote a high standard among Informatics Professionals in recognition of the impact that Informatics has on employment, business and society. CEPIS –which represents 36 Member Societies in 33 countries across greater Europe– has agreed on the following statement:

1. Background

Cloud Computing is not a very new concept in IT, in fact Cloud Computing is a more advanced version of the Data Processing Service Bureaus that we had 40 years ago. Nevertheless, the best known companies in the IT field offer or will shortly offer Cloud Computing services to a range of customers from organisations of all sizes to individuals. The biggest and best known Cloud Computing providers include Amazon with EC2 [5], Microsoft with Azure [6] and Google with GoogleApps (e.g. Gmail, Google Docs, Google Calendar) [7]. The paradigm of Cloud Computing can be described in simple terms as offering particular IT services that are hosted on the internet, the most common ones being Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a service (SaaS).

Cloud Computing is often marketed as an efficient and cheap solution that will replace the client-server paradigm. The paradigm shift involves/results in the loss of control over data as well as new security and privacy issues. For this reason caution is advised when deploying and using Cloud Computing in enterprises. After all, the first big issue in data protection in Europe arose at the end of the 1960's, when a Swedish company decided to have its data processing done by a service bureau in Germany and the data protection legislations in both countries were not alike.

With Cloud Computing rapidly gaining popularity, it is important to highlight the resulting risks. As security and privacy issues are most important, they should be addressed before Cloud Computing establishes an important market share. Many IT and important research agencies are aware of these risks and have produced reports and analyses to document them [1], [2], [3] ,[4].

2. Concerns

There seems to be no area of ICT that is not affected by Cloud Computing. Two main issues exist with security and privacy aspects of Cloud Computing:

1. loss of control over data and
2. dependence on the Cloud Computing provider.

These two issues can lead to a number of legal and security concerns related to infrastructure, identity management, access control, risk management, regulatory and legislative compliance, auditing and logging, integrity control as well as Cloud Computing provider dependent risks.

Typical issues due to the loss of control over data are:

1. Most customers are aware of the danger of letting data control out of their hands and storing data with an outside Cloud Computing provider. Data could be compromised by the Cloud Computing provider itself or other competitive enterprises which are customers with the same Cloud Computing provider. There is a lack of transparency for customers on how, when, why and where their data is processed. This is in opposition to the data protection requirement that customers know what happens with their data.
2. Many Cloud Computing providers are technically able to perform data mining techniques to analyse user data. This is a very sensitive function and even more so, as users are often storing and processing sensitive data when using Cloud Computing services. This holds especially true for social media applications that encourage users to share much of their private life e.g. private photos[1].
3. Mobile devices, in particular with their limited storage and computing capabilities are drivers for having services provided by Cloud Computing instead of using software on individual computers. Even data that are only to be transferred from one mobile device to another (local) device, are often transferred via the cloud, when cloud oriented applications on the mobile devices are involved. Therefore users often put themselves at risk without noticing this, as they assume that the data is transferred locally.
4. Since Cloud Computing is a service, it has to be accessed remotely. The connection between the Cloud Computing provider and customer is not always adequately protected. Security risks that threaten the transfer line include eavesdropping, DNS spoofing, and Denial-of-Service attacks.
5. The paradigm shift in Cloud computing makes the use of traditional risk management approaches hard or even impossible. Irrespective of the fact that control over data is transferred to the Cloud Computing provider, risk management and compliance issues are split between the Cloud Computing provider, Internet provider and customer. However, compliance can be seen as one of the important trust factors between the Cloud Computing provider and customer. Regulatory and legislative compliance is also problematic. Cloud data centres can be geographically dispersed. Therefore legislative compliance is not currently adequately defined.
6. As all technical control is given to the Cloud Computing provider, customers often want to have an external audit of this provider. Therefore logging and auditing information has to be stored and protected in order to enable verification. Appropriate logging could provide the possibility for forensic investigation in cases of incident.
7. Concerns also exist with regard to deletion of data: It is difficult to delete all copies of electronic material because it is difficult to find all copies. It is impossible to guarantee complete deletion of all copies of data. Therefore it is difficult to enforce mandatory deletion of data. However, mandatory deletion of data should be included into any forthcoming regulation of Cloud Computing services, but still it should not be relied on too much: the age of a "Guaranteed complete deletion of data", if it ever existed has passed. This needs to be considered, when data are gathered and stored.
8. Data Protection and Privacy legislation is not even similar in many countries around the globe yet Cloud Computing is a global service of the future. Consequently the problems and risks that affect data protection rules in Europe must be considered properly when Cloud Computing platforms are located on servers in non-European countries.
9. Cloud computing depends on a reliable and secure telecommunications network that assures and guarantees the operations of the terminal users of the services provided in the cloud by the cloud computing provider. Telecommunications networks are often provided separately from the Cloud computing services.

[1] More information on the special issues of social media applications can be found in the CEPIS statement on Social Networks – Problems of Security and Data Privacy [8].

Typical issues with regard to the dependence on the Cloud Computing provider are:

1. A major concern regarding dependence on a specific Cloud Computing provider is availability. If the Cloud Computing provider were to go bankrupt and stopped providing services, the customer could experience problems in accessing data and therefore potentially in business continuity.
2. Some widely used Cloud Computing services (e.g. GoogleDocs) do not include any contract between the customer and Cloud Computing provider. Therefore a customer does not have anything to refer to if incidents occur or any problems arise.
3. Cloud Computing is a service similar to other more “traditional” services and utilities (e.g. telecommunication, transaction banking, electricity, gas, water, etc.) Both Cloud Computing services and traditional services and utilities tend to be offered by large providers dealing with smaller customers. Therefore the customers usually depend on the providers because it is difficult to change providers if it is possible at all. Consequently traditional services (e.g. telecommunication, transaction banking, electricity, gas, water, etc.) are usually regulated with regard to the functionality range (e.g. mandatory functions, coverage), pricing, liability of the provider, and reliability.

Cloud Computing corroborates a trend that ICT security is no longer a purely technical issue but an issue between individuals and organisations and thus includes both human and organisational aspects such as management, contracting, and legal enforcement.

3. Recommendations

In particular the following points need to be considered.

1. Risk management and (legal) compliance issues must be well defined in the contract between Cloud Computing provider and customer and should enable transparency with regard to the processing and storage of data, e.g. the physical location of data storage. In this way the trust between the Cloud Computing provider and customer can be strengthened.
2. The service provided shall be compliant with the regulation and legislation that the customer needs to follow, and also customers should be enabled to be compliant with the respective regulation and legislation.
3. The problems and risks that affect data protection rules in Europe must be considered properly when Cloud Computing platforms are located on servers in non-European countries.
4. The communication line between the Cloud Computing provider and the customer has to be adequately protected to ensure confidentiality, integrity, authentication control and further to minimise the risk of denial-of-service attacks. An open and clear specification of the measurements taken to ensure the security of the communication line should be obligatory for any Cloud Computing provider and should be based on open and transparent standards and technologies.
5. The Cloud Computing providers should be obliged to ensure data confidentiality.
6. Mandatory deletion of data should be included into potential regulation of Cloud Computing services, but it should not be relied upon too much.
7. The fact that there is no guaranteed complete deletion of data needs to be considered, when data are gathered and stored.
8. In order to guarantee the availability of data, local backup of essential data by customers should be considered.
9. Development and better promotion of software that enables local data transfers between devices should be encouraged.
10. The telecommunications network that supports the cloud computing services should be secured and protected against malware and DOS attacks.

11. Adequate logging and auditing should be provided. An external audit can be beneficial for the reputation of the Cloud Computing providers as well as for strengthening the trust with the customer.
12. Non-professionals (e.g. the usual user) should be educated with regard to the new paradigm. Education should prepare them to make competent decisions on using Cloud Computing services including what information should be transferred into the Cloud and under what circumstances.
13. Professionals should be skilled to manage the new types of risks.
14. Given that some regulation will be needed in the future, e.g. to balance the power between providers and customers of Cloud Computing services, it would be wise to consider its weaknesses and issues before Cloud Computing becomes a critical service or infrastructure. It needs to be checked which of the dimensions of conflict and regulatory potential will be relevant (e.g. the guarantee and liability with regard to confidentiality and integrity of processed data). In particular when a Cloud Computing provider becomes part of a critical information infrastructure some regulation or limitations concerning their possible takeover by another party may be appropriate.
15. Research on the basic concepts and issues in informatics, security, and privacy and their consequences and trade-off's with regard to Cloud Computing should be encouraged. Also issues concerning the possible impact of Cloud Computing platforms on the validity of certification of applications that are certified according to criteria (e.g. Common Criteria, European Privacy Seal, etc.) may need to be investigated.

References

[1] J. Brodkin, Gartner: Seven cloud-computing security risks, available at: www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853.

[2] Cloud Computing Security Considerations, A Microsoft Perspective, Microsoft Whitepaper, 2010, available at: http://www.microsoft.com/malaysia/ea/whitepapers.aspx.

[3] Cloud Computing: Benefits, Risks and Recommendations for Information Security, ENISA Report, 2009, available at: www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

[4] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Cloud Security Alliance (CSA) Report, 2009, available at: www.cloudsecurityalliance.org/csaguide.pdf.

[5] Amazon Elastic Compute Cloud (Amazon EC2), http://aws.amazon.com/ec2/.

[6] Windows Azure platform, www.microsoft.com/windowsazure/.

[7] Google Apps, www.google.com/apps/

[8] CEPIS Statement, Social Networks – Problems of Security and Data Privacy, 2008, www.cepis.org/index.jsp?p=942&n=963#Social%20Networks