ISSN 2320 2629

Volume 3, No.5, September – October 2014

International Journal of Information Technology Infrastructure

Available Online at http://warse.org/pdfs/2014/ijiti01352014.pdf

Security Issues on Data Transfer Under Clouds – An Overview

M.Mohamed Sirajudeen[#1] and Dr. K. Subramanian[#2]

[#1] Department of Computer Science, J.J.College of Arts and Science, Pudukottai. {mdsirajudeen1@gmail.com}

[#2] Department of Computer Science, J.J.College of Arts and Science, Pudukottai. {subjjcit@gmail.com}

ABSTRACT

In general, according to user centric perception seems incompatible with the cloud. Whenever the Software as a Service (SaaS) environment is used, the service provider will be the responsible person for storage of data, in a way in which visibility and control is limited. So how can a consumer retain control over their data when it is stored and processed in the cloud? It will be a legal requirement and also something users/consumers want – it may even be necessary in some cases to provide adequate trust for consumers to switch to cloud services. There is a risk for the data stored or processed in the cloud may be put to unauthorized uses/access. It is part of the standard business model of cloud computing that the service provider may gain revenue from authorized secondary uses of users' data, most commonly the targeting of advertisements. However, some of the secondary data uses would be very unwelcome to the data owner or service providers.

Keywords: Service, cloud, advertise and unauthorized.

1. INTRODUCTION

The sixth one is "Transfer of data rights". It will not provide what rights in the data will be acquired by data processors and their sub-contractors, and whether these are transferable to other third parties upon bankruptcy, takeover, or merger [4][3].

2. RELATED WORK

2.1 SECURITY ISSUES IN THE ACCESS METHODS:

It will be a important one for the consumers and Cloud service providers in order to make legally binding agreements as to how data provided to Cloud Service Providers may be used. In the current trend, there are no technological barriers to the secondary uses. In future, there will be an agreements might be enforceable in a technological sense. This will help

The important factors for the lack of uses are: The first one, in cloud computing, the consumers' data is processed in 'the cloud' on machines they do not own or control, and there is a threat of theft, misuse especially for different purposes from those originally notified to and agreed with the consumer or unauthorized resale. The second one is "Access and transparency". It is difficult to control the exposure of the data transferred to the cloud, because information passing through some countries can be accessed by law enforcement agencies [1]. The third one is "Control over data lifecycle". It is not necessarily clear who controls retention of data or indeed what the regulatory requirements are in that respect as there can be a range of different data retention requirements, some of which may even be in conflict.

The fourth one is "Changing provider". It can also be difficult to get data back from the cloud, and avoid vendor lock-in. The fifth one is "Notification and redress". Uncertainties about notification, including of privacy breaches, and ability to obtain redress[8]. It can be difficult to know that privacy breaches have occurred and to determine who is at fault in such cases.

enhance trust and mitigate the effects of the blurring of security boundaries. In order to consider the factors that are influence with the security issues are: Unauthorized access [5][6] or disclosure in particular where the processing involves the transmission of data over a network, de destruction accidental or unlawful destruction or loss, Modification for inappropriate alteration, Unauthorized use for all other unlawful forms of processing. Cloud computing present's different risks to organizations than traditional IT solutions [9][10]. There are a number of security issues for cloud computing, some of which are new, some of which are exacerbated by cloud models, and others that are the same as in traditional service provision models. The security risks depend greatly upon the cloud service and deployment model. For example, private clouds can

to a certain extent guarantee security levels, but the economic costs associated with this approach are relatively high. At the network, host and application levels, security challenges associated with cloud computing are generally exacerbated by cloud computing but not specifically caused by it.

The main issues relate to defining which parties are responsible for which aspects of security. This division of responsibility is hampered by the fact that cloud Application Programming Interfaces are not yet standardized [11]. Customer data security raises a number of concerns, including the risk of loss, unauthorized collection and usage, and generally the Cloud Service Providers not adequately protecting data. It will be describe in the following figure 1.

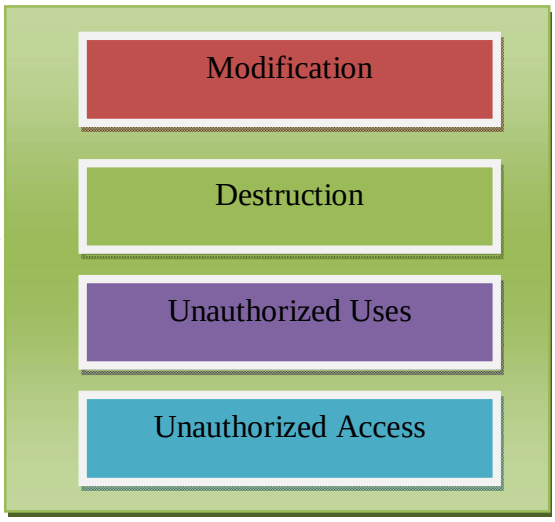

Figure 1. Components of Security issues

Abuse and immoral use could cover a wide variety of threats for example trying to use as much resource as possible (which could be quite high with a cloud model) without paying or in order to limit access for others.

3. OBSERVATIONS

At present the current cloud services pose an inherent challenge for the data privacy, because they typically result in data being present in unencrypted [12] form on a machine owned and operated by a different organization from the data owner. The major privacy issues relate to trust (for example, whether there is unauthorized secondary usage of Personal information uncertainty (ensuring that data has been properly destroyed, who controls retention of data, how to know that privacy breaches have occurred and how to determine fault in such cases) and compliance (in environments with data proliferation and global, dynamic flows, and addressing the difficulty in complying with trans border data flow requirements). When considering privacy risks in the cloud, as considered already within the introduction, context is very important as privacy threats differ according to the type of cloud scenario. For example, there are special laws concerning treatment of sensitive data, and data leakage and loss of privacy are of particular concern to users when sensitive data is processed in the cloud [2][7].

Currently this is so much of an issue that the public cloud model would not normally be adopted for this type of information. More generally, public cloud is the most dominant architecture when cost reduction is concerned, but relying on a cloud service provider (CSP) to manage and hold one's data in such an environment raises a great many privacy concerns [13]. Based on the observations for access of cloud services from the different security mechanism, the graph to be illustrated. It will be depicted in the figure 2.

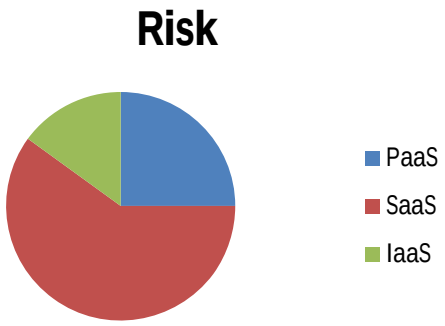

Figure 2. Risk Assessments for cloud access

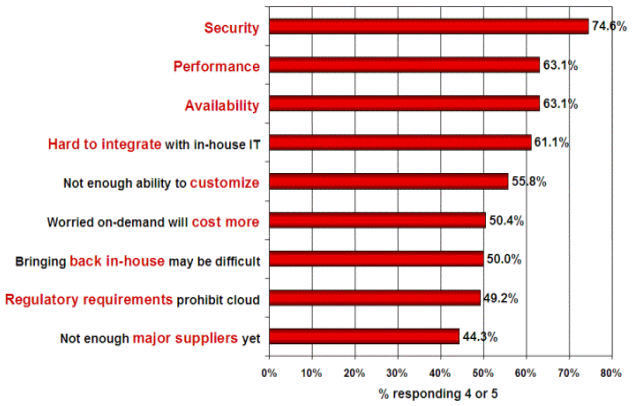

Figure 3. The challenges/issues which mainly affect the performance of Cloud Computing

The above statistical resulted graph (Figure 3) represents the results of the survey which was conducted by the IDC (International Data Corporation) in August, 2008 amongst senior business executives and IT professionals regarding the challenges/issues which mainly affect the performance of Cloud Computing. And the survey results show security at the top of the list which declares its importance compared to other parameters of Cloud Computing. During a keynote speech to the Brookings Institution policy forum, "Cloud Computing for Business and Society", Microsoft General Counsel Brad Smith also highlighted data from a survey commissioned by Microsoft for measuring attitudes on Cloud Computing among business leaders and the general population in January 2010. The survey found that while 58% of the general population and 86% of the senior business leaders are very much excited about the potential of Cloud Computing and more than 90% of these same people are very much concerned about the security, access and privacy of their own data in the Cloud [15]. The survey results show that the security is the major challenge amongst all the parameters that affect the performance and growth of Cloud Computing.

3.1 COMPONENTS OF THE SECURITY ISSUES

Even though, the virtualization and Cloud Computing delivers wide range of dynamic resources, the security concern is generally perceived as the huge issue in the Cloud which makes the users to resist themselves in adopting the technology of Cloud Computing. Some of the security issues in the Cloud are discussed below:

Integrity: Integrity makes sure that data held in a system is a proper representation of the data intended and that it has not been modified by an authorized person. When any application is running on a server, backup routine is configured so that it is safe in the event of a data-loss incident. Normally, the data will backup to any portable media on a regular basis which will then be stored in an off-site location [14].

Availability: Availability ensures that data processing resources are not made unavailable by malicious action. It is the simple idea that when a user tries to access something, it is available to be accessed. This is vital for mission critical systems. Availability for these systems is critical that companies have business continuity plans (BCP‟s) in order for their systems to have redundancy [14].

Confidentiality: Confidentiality ensures that data is not disclosed to unauthorized persons. Confidentiality loss occurs when data can be viewed or read by any individuals who are unauthorized to access it. Loss of confidentiality can occur physically or electronically. Physical confidential loss takes place through social engineering. Electronic confidentiality loss takes place when the clients and servers aren't encrypting their communications [14].

4. CONCLUSION

There are a number of security issues for cloud, and these depend upon the service provision and deployment models. A number of open issues remain, including audit. Availability may be an issue for public clouds- the future speed and global availability of network access required to use them may prevent widespread adoption in the short to medium term [5]. Overall, security need not necessarily suffer in moving to the cloud model, because there is scope for security to be outsourced to experts in security and hence in many cases greater protection than previously can be obtained. The major issues are probably to do with selection of service providers with suitable controls in place and to do with privacy, and are context- dependent.

REFERENCES

[1]. Mell P, Grance T (2009) A NIST definition of cloud computing. National Institute of Standards and Technology. NIST SP 800-145.http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf

[2]. IDC (2009) Enterprise Panel, September.http://www.slideshare.net/JorFigOr/cloud-computing-2010-an-idcupdate

[3]. Cloud Industry Forum (2011) Cloud UK: Adoption and Trends 2011.

[4]. Cloud Security Alliance (2010) Top Threats to Cloud Computing. v1.0,March.

[5]. Horrigan JB (2008) Use of cloud computing applications and services. Pew Internet & American Life project memo, Sept.

[6]. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT) (2001) Title V, s 505.

[7]. ENISA (2009) Cloud Computing: Benefits, risks and recommendations for information security. Daniele Catteddu and Giles Hogben (eds), November.

[8]. Marchini R (2010) Cloud Computing: A Practical Introduction to the Legal Issues. London: BSI.

[9]. McKinley PK, Samimi FA, Shapiro JK, Chiping T (2006). Service Clouds: A Distributed Infrastructure for Constructing Autonomic Communication Services. In: Dependable, Autonomic and Secure Computing, IEEE, 341-348.

[10].Warren S, Brandeis L (1890) The Right to Privacy. 4 Harvard Law Reviews 193.

[11].Westin A (1967) Privacy and Freedom. New York, USA, Atheneum.

[12].American Institute of Certified Public Accountants (AICPA) and CICA (2009) Generally Accepted Privacy Principles. August. http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/generallyacceptedprivacyprinciples/downloadabledocuments/gap _prac_%200909.pdf

[13].Solove DJ (2006) A Taxonomy of Privacy. University of PennyslavaniaLaw Review, 154(3):477, January.

[14]. Wood K, Pereira E. (Nov.2010) 'An Investigation into Cloud Configuration and Security', 2010 International Conference for Internet Technology and Secured Transactions, 1-6.

[15].http://www.microsoft.com/presspass/press/2010/jan10/1-20BrookingsPR.mspx.