ISSN 2320 - 2602
Volume 4 No.6, June 2015
International Journal of Advances in Computer Science and Technology
Available Online at http://www.warse.org/ijacst/static/pdf/file/ijacst01462015.pdf

Security and Authentication and Access on Data Transfer under the Cloud computing by using key

Saeed M. Hashim
M.Sc (Computer Science) ALqasim Green University, Iraq
seed19772003@gmail.com

ABSTRACT: Cloud storage moves the users data to big data centers, which are remotely located , on which user does not have any control . however , this unique feature of the cloud poses many new security challenges which need to be clearly understood and resolved. A scheme which gives a security the big data in the cloud which the customer can employ to check the correctness of his data in the cloud , by using key is provided.

Keywords: Cloud Computing, service, authentication, security.

1. INTROUDCTION

Cloud computing lets you access all your applications and documents from anywhere in the world, freeing you from the confines of the desktop and facilitating wholesale group collaboration. But cloud computing isn't for everyone; there are pros and cons to this type of web-based computing. Michael Miller explains which users can benefit from cloud applications and which should steer clear. Cloud computing represents a major change in how we store information and run applications[1]. Instead of hosting apps and data on an individual desktop computer, everything is hosted in the "cloud" an assemblage of computers and servers accessed via the Internet. This type of web-based computing frees you from the tyranny of desktop computing and opens up new forms of group collaboration. But as attractive as all that sounds, cloud computing isn't for everyone as figure 1.

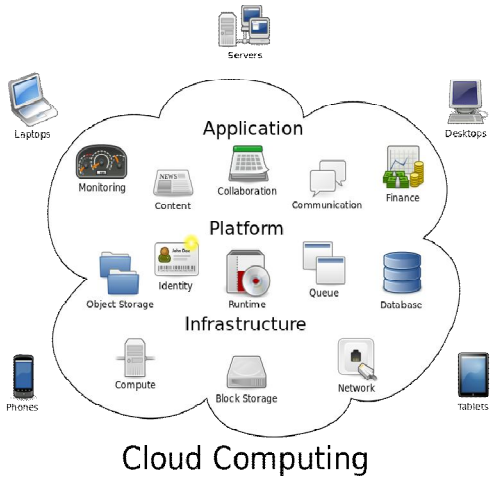

Figure 1: Cloud computing architecture regarding services

2. 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][2]. 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 on is “Notification and redress”. Uncertainties about notification, including of privacy breaches, and ability to obtain redress [3][4]. It can be difficult to know that privacy breaches have occurred and to determine who is at fault in such cases.

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 [5] 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 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 privacy are of particular concern to users when sensitive data is processed in the cloud [6][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 ones data in such an environment raises a great many privacy concerns . 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.

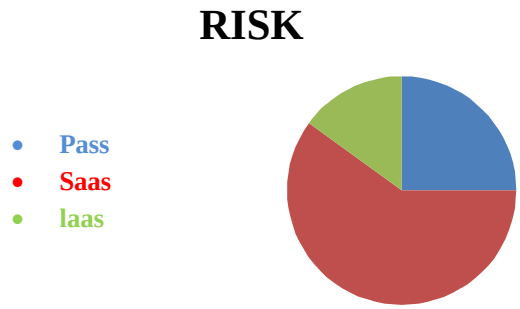

Figure 2. Risk Assessments for cloud access

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 [8]. 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 leader 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 [9]. The survey results show that the security is the major challenge amongst all the parameters that affect the performance and growth of cloud computing.

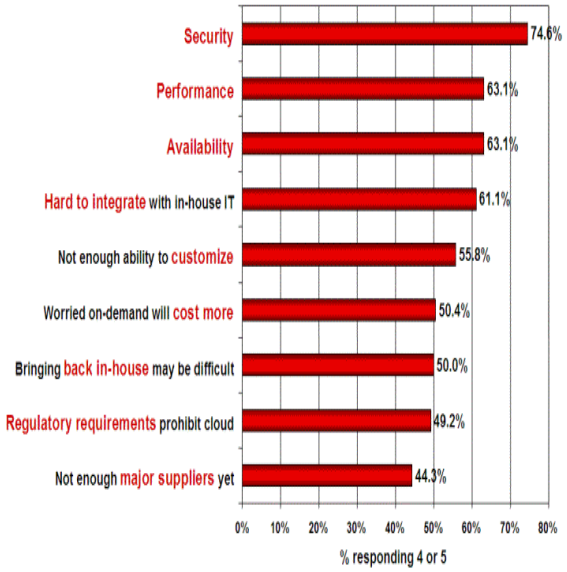

Figure 3. The challenges / issues which mainly affect the performance of cloud computing

4. 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 [10].

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 [11].

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 [12].

5. 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. 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 Institite of Standards and Technology . NIST SP 800- 145 http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf.

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

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

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

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

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

[7]. McKinley PK, Sammie 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.

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

[9]. Westin A (1967) Privacy and Freedom. New York, USA, Athenaeum .

[10]. 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.

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

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