IJCSN International Journal of Computer Science and Network, Volume 4, Issue 5, October 2015
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 0.417

Possible Improvement Directions in Cloud Computing

Tariq Ahamad

College of Computer Engineering & Sciences, Prince Sattam Bin Abdulaziz University, KSA

Abstract - Cloud computing is the most emerging trend in modern world technology and has its meaning to different people under different circumstances. But the most common characteristics are secure on demand access to different services and transfer of data from both sides of the organization. As the number of services, tools and active organizations is increasing, so is increasing the threats. Most of the securities have drawbacks in terms of cost and reliability for both cloud computing organizations and its using organizations. In this research article, we categorize the basic problems that are related to security and must be dealt seriously.

Keywords - *Cloud Computing, Access Control, PAAS, SAAS, IAAS.*

1. Introduction

Cloud computing simply refer to remote access to store , process and manage data on remote servers rather than local computer or server. Cloud is all about computer services, not products. Cloud computing is a general term for anything that involves delivering hosted services over the Internet. Cloud computing is not a technology but a model of provision and marketing IT services that meet certain characteristics [1]. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) explained in the following figure 1.

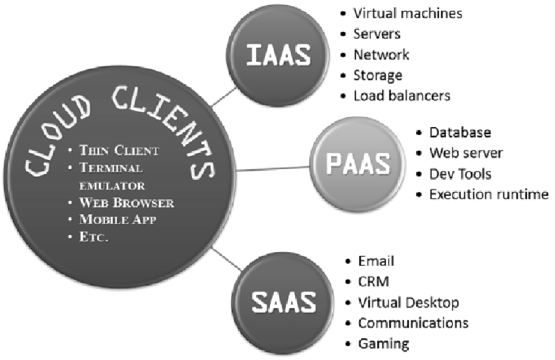

Figure 1. Cloud Computing Services

The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flowcharts and diagrams [2].

A cloud service has three distinct characteristics that differentiate it from traditional hosting [3]. It is sold on demand, typically by the minute or the hour; it is elastic -- a user can have as much or as little of a service as they want at any given time; and the service is fully managed by the provider (the consumer needs nothing but a personal computer and Internet access). Significant innovations in virtualization and distributed computing, as well as improved access to high-speed Internet and a weak economy, have accelerated interest in cloud computing.

A cloud can be private or public. A public cloud sells services to anyone on the Internet. (Currently, Amazon Web Services is the largest public cloud provider.) A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people [4]. When a service provider uses public cloud resources to create their private cloud, the result is called a virtual private cloud [5]. Private or public, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services.

2. Security Issues in Cloud Computing

1. If we consider Google or Microsoft, many accounts are currently running and new accounts are created using their websites to communicate with security and privacy. Usually we never think who secures our account and data , and where is our data stored. Different kinds of data with different privacy are stored in those mail accounts and every site has got its own server to keep it secure and manage the data.

2. After all the security tools and promises, an account can be hacked from any part of the world , what is the reason? This is a major issue and can be created and caused by the person we trust or the networking around us. And if these are the issues with the server

then that is not the issue as the server will never hack your account.

3. Where is the data stored? Since we know that our contacts and emails are stored and managed by servers but we don't know on which server and the reason is that we don't understand or know about the complete service or application that has been created by the service provider (like Google, or Microsoft) for our use.

3. Common Threats in Cloud Computing

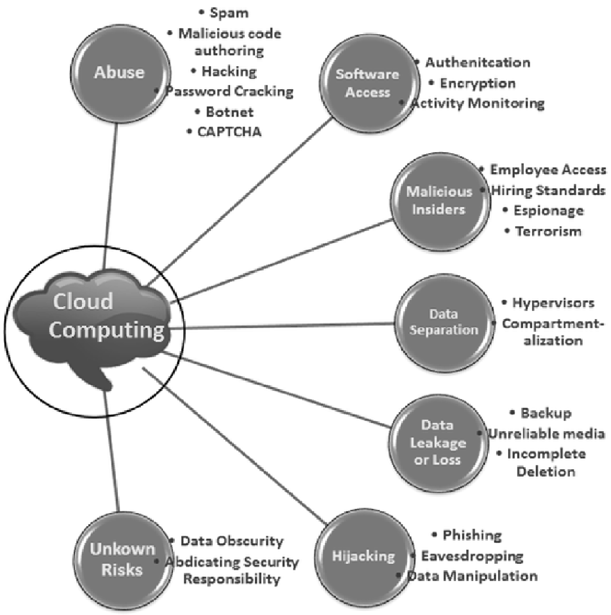

Figure 2 - Cloud Computing Threats

1. DDoS
2. Malicious intruders and insiders
3. Shared tech. issues
4. Reliability (data leakage or less)
5. Hacking (both service and account)

4. In Search of Possible Solution

In this research article we are not about to propose the solution to these problems. Instead we merely try to point out at few capable directions in which a better solution can be found.

a. *Monitor auditing.* In this approach we consider a pre installed reliable monitor at cloud server that can monitor and audit the basic tasks and operations of the server (cloud server). Once data owner wants to access the data, the installed trusted monitor will send proofs of compliance confirming that specific access rules and policies haven't been violated. To ensure the true integrity of installed monitor, its secure bootstrapping is executed and run beside the operating system and applications. The installed trusted monitor can enforce all types of access policies and can perform auditing and monitoring tasks. The code of the trusted monitor along with statement of compliance that is produced by the monitor is signed in order to produce proof of compliance. On the reception of this proof of compliance by the data owner, it can easily verify that the true and correct code has been executed and run , and the cloud server has complied and followed all the access control policies.

b. *Encryption of cloud data:* Another approach that can be followed in order to secure data on cloud is the encryption of data on cloud but the only problem with this is that it limits the data use because the main two processes of data i.e. searching and indexing becomes difficult to execute. For example, if we store data as normal text , one can easily and efficiently search the data with a specified word but if the data is encrypted, it becomes impossible to search with traditional and randomized encryption techniques. There are new tools and techniques that can solve this problem, recently cryptographers have invented new versatile encryption technique that allows different operation on hyper and cy[her text.

5. Conclusion

Cloud computing, the more it grows the more trust and reliability and security is expected and needed. In the research, we have proposed two different ideas that can be used to develop and maintain the trust and reliability in order to make cloud data more safe. We suggest two ideas involving monitor auditing and advanced encryption of cloud data to ensure better and reliable access control policies.

Acknowledgement

The research was conducted at Prince Sattam bin Abdulaziz University, Al-Kharj, Saudi Arabia.

References

[1] Gartner (2012) Cloud Computing. Retrieved April 15, 2012 from http:/ /www. gartner.com /technology/it-glossary /cloud-computing.jsp

[2] Rhoton, J. (2011). Common Definition. Cloud Computing Explained: Second Edition. Recursive Press, US.

[3] Microsoft Corporation (2011) Addressing Cloud Computing Security Considerations. Retrieved April 2,

2012 from http://search .microsoft.com/en-s/results.aspx?form=MSHOME &setlang=enus&q=Addressing%20Cloud%20 Computing%20Security%20Considerations .

[4] Bloomberg, J. (2012) Why Public Clouds are More Secure than Private Clouds. Retrieved March 2, 2012 from http://www.zapthink.com/ 2012/02/07/why-public- clouds-are-more-secure-than-private-clouds/

[5] Jansen et al (2011) Public Cloud Computing. Retrieved April 1, 2012 from http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

[6] Beckham, J. (2011) The Top 5 Security Risks of Cloud Computing. Retrieved February17, 2012 from http://blogs.cisco.com/smallbusiness/the-top-5-security-risks-of-cloud- computing/