CLOUD SECURITY – A SHORT PRIMER

Joel-Ahmed M. Mondol

Dept. of Electrical and Computer Engineering, College of Engineering, University of Saskatchewan, 57 Campus Dr, Saskatoon, SK, S7N 3R2, Canada, email:joel.ahmed@usask.ca

ABSTRACT

Security is of utmost concern in cloud computing environment. Without a guarantee of acceptable security, clients are reluctant to accept cloud computing as a solution to their enterprise and personal computation need. The large adaptation that is required to transform cloud computing from a buzz word to a reliable and acceptable standard in corporate and client computing is still out of reach due to security and privacy concerns. This short paper provides a primer on cloud security concerns and scrutinizing the solutions that address those concerns.

1. INTRODUCTION

Cloud computation is a paradigm shift [1] in the general computing industry. Starting from consumer level applications to enterprise level infrastructure development, deployment and management, cloud computing allows massive innovation to take place and ensure scales of economy in a multitude of services. Cloud computing technology not only reduces client expenditure, it also changes deployment, distribution and availability landscape for computing service providers and system developers.

2. CLOUD MARKET GROWTH

Hickey in his survey states that by 2013, there will be $44.2 billion spent on cloud computing services [2][3]. A cloud user survey conducted by research group IDC [4] have found over 75% of participants have interest in cloud computing due to the potential of paying only for what is used, easy / fast deployment to end users and monthly payments. A majority of the respondents have shown interest in the collaborative aspect of applications in cloud computing. Data backup, productivity apps, storage capacity on demand, IT management software, server capacity, business apps (CRM, HR, ERP) were other reasons for pursuing cloud computing . However when it came to challenges and concerns: security, availability, performance and on – demand payment model costing more over the long run were some of the concerns identified by the survey.

3. CLOUD ARCHITECTURE & SECURITY

Security is a prerequisite in cloud computing infrastructure. It is essential to ensure that only authorized access is allowed [5]. Computation and information interchange greatly depends on trust. Security concerns are huge impediments for cloud computing to become the primary computation resource.

With regards to security the problem is with control, availability and computation of the data. Security breaches can impact clients data at any point of time which possibly can put the client into an uncomfortable legal situation. Security concerns of this magnitude are not present in a non-cloud desktop or client – server environment. At the end adaptation of cloud computing is essentially a weighted decision based on operational impact and risk averseness towards data security versus the benefits of cloud computing.

Table I presents different security requirements required by different user groups. Notice that different cloud architecture layers have different levels of security requirement based on the users or user groups that they are trying to secure.

4. CLOUD SECURITY SOLUTIONS

Security researchers at the Black Hat USA security conference in Las Vegas showed how users of Amazon's Elastic Compute Cloud (EC2) services were tricked into using virtual machines that could have included "back doors" for snooping [6].

Table I: User Specific Security Requirements [7]

Level	Users	Security Requirement
App Level (SAAS)	End client applies to person or organization who subscribes to a service offered by cloud provider and is accountable for its use	• Privacy in multitenant environment • Data protection from exposure (remnants) • Access control • Communication protection • Software security • Service availability
Virtual Level (PAAS)	Developer–moderator applies to a person or organization that deploys software on the cloud	• Access control • Application security • Data security (data in transit, data at rest, remnant) • Secure Images • Virtual cloud protection • Communication security

Traditional security practices will still play a role in the cloud based computing but they are not enough to take care of the challenges due to de-perimeterization. Experts feel that security needs to be implemented at a component level like encryption of any data present in the Cloud (a point highlighted by Dan Kaminsky at Cloud Camp Seattle), secure communications and data level

978-1-4673-0382-8/12/$31.00 ©2012 IEEE

authentication. A comprehensive cloud computing security framework may finally encourage the enterprises towards the cloud [8].

Brodkin shows that according to the analyst firm Gartner there are seven specific security issues in cloud computing. They have suggested that prior to jumping on the cloud computing platform; customers should raise concerns with respect to privileged user access, regulatory compliance, data location, data segregation, recovery, long term viability and investigative support [9]. Some of the different security solutions as provided by some of the major cloud service providers are listed in Table II [10]:

Table II: Cloud Vendors and their security solution [10]

Vendor	Security Solution
AWS	AWS Secret Access Key, Type II certification firewall, X.509 certificate
GoGrid	Secure VLAN Management, Primecloud Service for hosted private cloud
Rackspace cloud	Encrypted communication channel, API Access Key, session authentication token
GAE	Google Secure Data Connector, TLS based Server authentication
GigaSpaces	Amazon security groups, built in SSH tunneling
Azure	Security Assertion Markup
SunCloud	Process and user rights management
Salesforce	Users and security programmatic and platform security framework.

The process of a federated identification mechanism is critical for the Cloud. The Cloud Security Alliance (CSA) group has identified security flaws and its remediation within different service models. Table III provides a summarized version of some of the remediation's they have provided [11]. Although not complete, it gives an understanding where the threats are and how they can be resolved within the CSA model.

Table III: Cloud Security Flaws & remediation [11]

Threats	Remediation	CSA Domain
Abuse and Nefarious Use of Cloud Computing	• Stricter initial registration and validation processes. • Enhanced credit card fraud monitoring and coordination.	8: Data Center Operations 9: Incident Response, Notification and Remediation
Insecure Interfaces and APIs	• Analyze the security model of cloud provider interfaces.	10: Application Security
Malicious Insiders	• Specify HR requirements as part of legal contracts. • Determine security breach notification processes.	2:Enterprise Risk Management 7: Traditional Security, Business Continuity
Shared Technology Issues	• Implement security best practices for installation/configuration.	8: Data Center Operations 13: Virtualization
Data Loss or Leakage	• Implement strong API access control. • Protect integrity of data in transit.	5: Information Lifecycle 11: Encryption 12: Identity

5. CONCLUSION

Due to the open nature of the web – all data to be stored, maintained and processed in the cloud should be secured. At the same time authentication and authorization are core ingredients in the security infrastructure for the cloud. Following are some security recommendations and insights from this short primer:

1. Data stored in the cloud must be encrypted.
2. Effective and robust security model is created when both client and vendors are involved
3. Prior to deploying on the cloud, data & identity management strategy should be created
4. A distributed operation and federated identity management scheme can prove to be inexpensive and readily deployable.
5. Regulatory and legislative compliance.

REFERENCES

[1] B. Hayes, "Cloud computing," ACM DL Digital Library, vol. 51, no. 7, pp. 9-10, July 2008.

[2] M. Ahmed, "Security Risks of Cloud Computing and Its Emergence as 5th Utility Service," Comm. in Comp and Inform Science, vol. 76, pp. 209-219, 2010.

[3] A. R. Hickey, "Cloud-computing-security-risks-outweigh-benefits-survey," 09 August 2010. [Online]. Available:www.crn.com/news/security/224202475/cloud-computing-security-risks-outweigh-benefits-survey.htm [Accessed 12 February 2011].

[4] IDC Exchange, 2010. [Online]. Available: blogs.idc.com/ie/?p=730.

[5] NIST: 800 - 145, "The NIST definition of cloud computing," September 2011.

[6] March 2011. [Online]. Available: http://cachef.ft.com/cms/s/2/6cc04ca2-7f8e-11de-85dc-00144feabdc0.html#axzz1GdOk95LT.

[7] D. L. Dimitrios Zissis, "Addressing cloud computing security issues," Future Gen Comp Systems, Dec 2010.

[8] K. Subramanian, March 2009. [Online]. Available: www.cloudave.com/2307/cloud-computing-security-framework-may-nudge-the-enterprises-towards-clouds/.

[9] J. Brodkin, Available : http:// www.infoworld.com /print/ 36853. [Accessed 12 Feb 2011].

[10] E. C. I. L. Bhaskar Prasad Rimal, "A Taxonomy, Survey, and Issues of Cloud Computing Ecosystems," Comp Comm and Networks, vol. 0, pp. 21 - 46, 2010.

[11] M. Litoiu, M. Woodside, J. Wong, J. Ng and G. Iszlai, "A business driven cloud optimization architecture," in Proceedings of the 2010 ACM Symposium on App Comp, Sierre Switzerland, 2010.