Survey on Security Openness and Heedfulness in Cloud Computing Environment

Vivekanandhan M.
Software Programmer
India

ABSTRACT
Cloud computing is a fastest growing technology in recent years. Cloud computing holds the potential to eliminate the requirements for setting up of high-cost computing infrastructure for IT-based solutions and services that the industry uses. Cloud services are becoming an essential part of many organizations. It promises to provide a flexible IT architecture, accessible through internet from lightweight portable devices. In a cloud computing environment, the entire data resides over a set of networked resources, enabling the data to be accessed through virtual machines. Cloud providers have to adhere to security and privacy policies to ensure their users' data remains confidential and secure. Though there are some ongoing efforts on developing cloud security standards, most cloud providers are implementing a mish- mash of security and privacy controls. This extensive survey paper aims to elaborate and analyze the populous vacillating issues threatening the cloud computing environment.

Keywords
Cloud Computing, Security, Authentication, Saas, Paas, Iaas

1. INTRODUCTION
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (This definition is from the latest draft of the NIST Working Definition of Cloud Computing published by the U.S. Government's National Institute of Standards and Technology.)

One of the most important features of cloud is its elasticity, which allows the user to pay as per their needs. While cloud is beneficial in terms of economy and availability but organizations can't ignore the security threats to their data on cloud storage. Due to the security issues in cloud many users are reluctant to use it for personal and sensitive data storage. Since cloud storage is third party storage it needs special data security solutions, than traditional third party storages[1].

Internet has been a driving force towards the various technologies that have been developed since its inception. Arguably, one of the most discussed among all of them is Cloud Computing. Over the last few years, cloud computing paradigm has witnessed an enormous shift towards its adoption and it has become a trend in the information technology space as it promises significant cost reductions and new business potential to its users and providers The advantages of using cloud computing include: i) reduced hardware and maintenance cost, ii) accessibility around the globe, and iii) flexibility and highly automated processes wherein the customer need not worry about mundane concerns like software up-gradation A plethora of definitions have been given explaining the cloud computing. Cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. In such an environment users need not own the infrastructure for various computing services. In fact, they can be accessed from any computer in any part of the world. This integrates features supporting high scalability and multi-tenancy, offering enhanced flexibility in comparison to the earlier existing computing methodologies. It can deploy, allocate or reallocate resources dynamically with an ability to continuously monitor their performance[2].

2. SCRUTINY ON ISSUES IN EXISTING CLOUD COMPUTER ENVIRONMENT
Acklyn Murray, Geremew Begna, Ebelechukwu Nwafor, Jeremy Blackstone, Wayne Patterson Department of Systems and Computer Science of Howard University proposed "Cloud Service Security & Application Vulnerability "that Cloud computing model offers so many benefits yet it faces issues and criticism due to its non-stringent security enforcement. There should be stricter security policies put in place when dealing with cloud applications. Also, applications should enforce more layers of security such as 2 factor authentication to ensure that data is properly secured. Data at rest or in transit should be encrypted and signed to ensure confidentiality, integrity. Also, most business organizations should employ a hybrid cloud model since this ensures that personal information is managed internally on private clouds and not stored on public clouds. This helps to alleviate the risk of personal information being compromised [3].

Previous studies have attempted to determine cloud security issues. Popović et al.'s study on cloud security controls and standards has been focused primarily at the provider end and concentrated on cloud engineering. Subashini and Kavitha present a survey of the different security risks to the cloud. This study is specific to the security issues due to the cloud service delivery models. Kamongi et. al. have also developed a risk model for the cloud but haven't tied it with existing compliance standards[4].

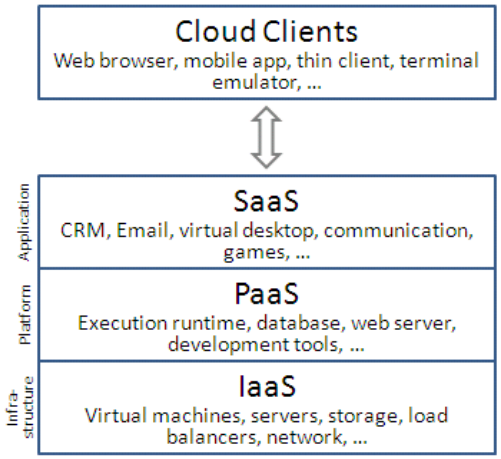

Figure1: Cloud Computing Architecture

Table 1. Cloud Computing Service Providers on Cloud Service Models

Cloud Service Models	Cloud Service Providers
SaaS	Antenna Software, Cloud9 Analytics, CVM Solutions, Exoprise Systems, Gageln, Host Analytics, Knowledge Tree, LiveOps, Reval, Taleo, NetSuite, Google Apps, Microsoft 365, Salesforce.com, Rackspace, IBM, and Joyent
PaaS	Amazon AWS, Google Apps, Microsoft Azure, SAP, SalesForce, Intuit, NetSuite, IBM, WorkXpress, and Joyent
IaaS	Amazon Elastic Compute Cloud, Rackspace, Bluelock, CSC, GoGrid, IBM, OpenStack, Rackspace, Savvis, VMware, Terremark, Citrix, Joyent, and BluePoint

Identification is a basic and first process of establishing and distinguishing amongst person/ user & admin ids, a program/ process/ another computer ids, and data connections and communications. Often we use alphanumerical string as user identification key and some may use your email as the user identification key and this can be checked against when a user login into the system.

Authentication and authorization are two distinct forms of access controls to access any information in the system. Privacy is the key to maintaining the success of cloud computing and its impact on sharing information for social networking and team work on a specific project. This can be maintained by allowing users to choose when and what they wish to share in addition to allowing encryption and decryption facilities when they need to protect specific information/ data/ media content.

Integrity is the basic feature of human being as a process of maintaining consistency of actions, communications, values, methods, measures, principles, expectations, and outcomes. Ethical values are important for cloud service providers to protect integrity of cloud user's data with honesty, truthfulness and accuracy at all time. In cloud computing terms, we can achieve integrity by maintaining regular redundancy checks and digital certification in addition to other basic security features of maintaining identification, authentication, and authorization [5].

Durability is also known as, persistency of user actions and services in use should include sessions and multiple sessions.

Cloud computing model offers so many benefits yet it faces issues and criticism due to its non-stringent security enforcement. There should be stricter security policies put in place when dealing with cloud applications. Also, applications should enforce more layers of security such as 2 factor authentication to ensure that data is properly secured. Data at rest or in transit should be encrypted and signed to ensure confidentiality, integrity. Also, most business organizations should employ a hybrid cloud model since this ensures that personal information is managed internally on private clouds and not stored on public clouds. This helps to alleviate the risk of personal information being compromised [6].

3. COUNTER MEASURES

A cloud computing infrastructure includes a cloud service provider, which provides computing resources to cloud end users who consume those resources. In order to assure the best quality of service, the providers are responsible for ensuring the cloud environment is secure. This can be done by defining stringent security policies and by applying advanced security technologies.

3.1. Security policy enhancement

With a valid credit card, anyone can register to utilize resources offered by cloud service providers. This causes hackers to take advantage of the powerful computing power of clouds to conduct malicious activities, such as spamming and attacking other computing systems. By mitigating such abuse behavior caused by weak registration systems, credit card fraud monitoring and block of public black lists could be applied [7]. Also, implementation of security policies can reduce the risk of abuse use of cloud computational power [8]. Well-established rules and regulations can help network administrators manage the clouds more effectively. For example, Amazon has defined a clear user's policy and isolates (or even terminates) any offending instances whenever they receive a complaint of spam or malware coming through Amazon EC2 [9].

3.2 Access management

The end users' data stored in the cloud is sensitive and private; and access control mechanisms could be applied to ensure only authorized users can have access to their data. Not only do the physical computing systems (where data is stored) have to be continuously monitored, the traffic access to the data should be restricted by security techniques. Firewalls and intrusion detection systems are common tools that are used to restrict access from untrusted resources and to monitor malicious activities. In addition, authentication standards, Security Assertion Markup Language (SAML) and eXtensible Access Control Markup Language (XACML), can be used to control access to cloud applications and data. SAML focuses on the means for transferring authentication and authorization decisions between cooperating entities, while XACML focuses on the mechanism for arriving at authorization decisions [10].

3.3 Data protection

Data breaches caused by insiders could be either accidental or intentional. Since it is difficult to identify the insiders' behavior, it is better to apply proper security tools to deal with insider threats. The tools include: data loss prevention systems, anomalous behavior pattern detection tools, format preserving and encryption tools, user behavior profiling, decoy technology, and authentication and authorization technologies. These tools provide functions such as real-time detection on monitoring traffic, audit trails recording for future forensics, and trapping malicious activity into decoy documents.

4. CONCLUSION

Cloud computing, in the recent years, has taken the ability to prove its necessity in terms of data outsourcing. But it also poses a threat to the data owner in terms of privacy and security of data. As Cloud Computing becomes prevalent, more and more sensitive information are being centralized into the cloud, such as e-mails, personal health records, company finance data, and government documents, etc. The fact that data owners and cloud server are no longer in the same trusted domain may put the outsourced unencrypted data at risk. The cloud server may leak data information to unauthorized entities or even be hacked. Although Cloud computing can be seen as a new phenomenon which is set to revolutionize the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. This paper helps to identify cloud computing is and what are the challenges and the issues relating to the cloud computing [11].

As part of our ongoing work, we are further analyzing other IT Security Issues in cloud paradigm and determine if they should be incorporated into our cloud security application.

5. ACKNOWLEDGMENTS

This Technical paper could not have been written without my parents and my mentors Irfan, Remya and Uday, Saravana who encouraged and challenged me through my professional career. And giving me the strength to reach for the stars and chase my dreams, and authors mentioned in the reference.

6. REFERENCES

[1] W. A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," 44th Hawaii International Conference on System Sciences, pp. 1–10, Koloa, Hawaii, January 2011.

[2] K. Zunnurhain and S. Vrbsky, "Security Attacks and Solutions in Clouds," 2nd IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, December 2010.

[3] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On Technical Security Issues in Cloud Computing," IEEE International Conference in Cloud Computing, pp. 109-116, Bangalore, 2009.

[4] DataLossDB Open Security Foundation. http://datalossdb.org/statistics

[5] A. Tripathi and A. Mishra, "Cloud Computing Security Considerations Interface," 2011 IEEE International Conference on Signal Processing, Communications and Computing, Xi'an, China, September 2011.

[6] D. Catteddu and G. Hogben, "Cloud Computing Benefits, Risks and Recommendations for Information Security," The European Network and Information Security Agency (ENISA), November 2009.

[7] Sophos Security Threat Report 2012. http://www.sophos.com/

[8] Symantec Internet Security Threat Report, 2011 Trends, Vol. 17, April 2012.

[9] M. McIntosh and P. Austel, "XML Signature Element Wrapping Attacks and Countermeasures," 2005 workshop on Secure web services, ACM Press, New York, NY, pp. 20–27, 2005.

[10] Web Based Attacks, Symantec White Paper, February 2009.

[11] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Special Publication 800-144, December 2011.

[12] Justin LeJeune, Cara Tunstall, Kuo-pao Yang and Ihssan Alkadi, CSIT Department at SLU "An Algorithmic Approach to Improving Cloud Security: The MIST and Malachi Algorithms", 978-1-4673-7676 ,2016 IEEE

[13] Victor Chang, Muthu Ramachandran, Member, IEEE "Towards achieving Data Security with the Cloud Computing Adoption Framework", 2015,IEEE

[14] Amit Hendre and Karuna Pande Joshi CSEE Department, University of Maryland Baltimore County Baltimore, MD, USA "A Semantic Approach to Cloud Security and Compliance" 2015 IEEE

[15] H. C. Li, P. H. Liang, J. M. Yang, and S. J. Chen, "Analysis on Cloud-Based Security Vulnerability Assessment," IEEE International Conference on E-Business Engineering, pp.490-494, November 2010.

[16] Vahid Ashktorab , Seyed Reza Taghizadeh "Security Threats and Countermeasures in Cloud Computing Volume 1, Issue 2, October 2012

[17] Cloud Security Risks and Solutions," White Paper, BalaBit IT Security, July 2010.

[18] S. J. Stolfo, M. B. Salem, and A. D. Keromytis, "Fog computing: Mitigating Insider Data Theft Attacks in the Cloud," IEEE Symposium on Security and Privacy Workshops, pp. 125-128, San Francisco, CA, 2012.

[19] M. Jensen, C. Meyer, J. Somorovsky, and J. Schwenk, "On the Effectiveness of XML Schema Validation for Countering XML Signature Wrapping Attacks," First International Workshop on Securing Services on the Cloud, Milan, Italy, September 2011

[20] N. Provos, M. A. Rajab, and P. Mavrommatis, "Cybercrime 2.0: When the Cloud Turns Dark," ACM Communications, Vol. 52, No. 4, pp. 42–47, 2009.

[21] Insider Threats Related to Cloud Computing, CERT, July 2012. http://www.cert.org/

[22] D. Jamil and H. Zaki, "Security Issues in Cloud Computing and Countermeasures," International Journal

of Engineering Science and Technology, Vol. 3 No. 4, pp. 2672-2676, April 2011.

[23] S. S. Rajan, Cloud Security Series | SQL Injection and SaaS, Cloud Computing Journal, November 2010.

[24] P. P. Ramgonda and R. R. Mudholkar, "Cloud Market Cogitation and Techniques to Averting SQL Injection for University Cloud," International Journal of Computer Technology and Applications, Vol. 3, No. 3, pp. 1217-1224, January, 2012.

[25] T. Roth, "Breaking Encryptions Using GPU Accelerated Cloud Instances," Black Hat Technical Security Conference, 2011.

[26] Prince Jain Malwa Polytechnic College Faridkot, Punjab-151203, India "Security Issues and their Solution in Cloud Computing" International Journal of Computing & Business Research ISSN (Online): 2229-6166

[27] Krishna Prakash and Balachandra "security issues and challenges in mobile computing and m-commerce" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.2, April 2015

[28] Abdullah , Imran, Fida Hussain "The Secure Data Storage in Mobile Cloud Computing"

[29] Computer Engineering and Intelligent Systems www.iiste.org ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.6, No.5,2015

[30] A. S. Choudhary and M. L. Dhore, "CIDT: Detection of Malicious Code Injection Attacks on Web Application," International Journal of Computer Applications, Vol. 52, No. 2, pp. 19-26, August 2012.

[31] Web Application Attack Report For The Second Quarter of 2012 http://www.firehost.com/company/newsroom/web-application-attack-report-second-quarter-2012

[32] Visitors to Sony PlayStation Website at Risk of Malware Infection, July 2008. http://www.sophos.com/en-us/press-office/press-releases/2008/07/playstation.aspx

[33] 2012 Has Delivered Her First Giant Data Breach, January 2012. http://www.infosecisland.com/blogview/19432-2012-Has-Delivered-Her-First-Giant-Data-Breach.html

[34] N. Gruschka and L. L. Iacono, "Vulnerable Cloud: SOAP Message Security Validation Revisited," IEEE International Conference on Web Services, Los Angeles, 2009.

[35] Tackling the Insider Threat http://www.bankinfosecurity.com/blogs.php?postID=140

[36]