Special Issue of Engineering and Scientific International Journal ISSN 2394-7187(Online) ISSN 2394-7179 (Print)
Proceedings of the UGC Sponsored - National Conference on "Recent Statistical Computing Techniques and their Applications"
Department of Statistics and Department of Computer Science, Ramanujan College,University of Delhi, Delhi.
March 11-12, 2016. ***Published on January 2017***

Study on the Development of Cloud Security

Jitendra Singh[#1], Kamlesh Raghuvanshi[*2]
[1]*Associate Professor, Computer Science Department, Bhagani Nivedita College, University of Delhi-43*
[2]*Assistant Professor, Computer Science Department, Ramanujan College, University of Delhi-19*

Abstract— Security is a critical issue in cloud computing. Despite of tremendous growth in cloud adoption, it is still prevalent in cloud paradigm. As a result, addressing security issue is equally important for the industry as well as academia. Several measures have already been initiated to strengthen the cloud security. However, contribution is limited in the form of draft, reports, recommendation and research article in order to improve the cloud security. This work is an attempt to discover the various methods employed by the industry and academia to identify and bridge the security gaps based on various types of security threats prevailing in this promising paradigm. Major cloud security tools with their functionality and employed methods to secure the cloud have been reviewed. Contribution of academia has been highlighted and the gaps thereof have been further discussed.

Keywords— *Cloud Security; Security Tools; Major Cloud Threats; Cloud Security Group.*

1. Introduction

According to IDC research, the upcoming decade is set to be dominated by Social media, Mobile phones, Analytics and Cloud computing which is widely known as SMAC[1]. In these four paradigms, cloud computing is set to change the way IT is procured and utilized. Cloud computing is defined by many experts in this area, for instance [2] has done the complete listing of cloud definitions from various experts. However, the one widely popular is suggested by NIST[3].

Research majors such as Gartner, IDC, and Aberdeen etc. have predicted huge growth for the cloud paradigm. Fortunately, cloud paradigm has already surpassed many of the predicted figures of its growth[32-33]. Realizing this huge growth potential many cloud vendors small and big have already emerged and more new vendors are continuing to emerge[31-33].

Agility, shareability and on demand usage of resources are some of the significant advantages of cloud computing [3, 4, 5]. Cloud computing supports wide variety of devices including desktop, laptop, Smartphones, tablets etc. for accessing and usage of data. Subscribers can access the data from anywhere and anytime using these devices. This ease of usage has also led to the generation of many challenges related to data security and accessibility. Since, cloud resources can be subscribed and utilized by any users irrespective of his expertise in technology domain, as a result unskilled users using the same device to access the cloud resources as well as accessing the other internet activities. All such activities have led to generation of great risk in cloud resources that is centrally located.

Cloud computing is widely appreciated and adopted by SME's which are lacking the upfront investment and dedicated expert teams for development and maintenance. Despite of aforementioned positive side, cloud computing is facing the challenges from various fronts including security, interoperability, SLA etc. According to various reports published, security has been cited as the major threat to cloud computing and acting as key component in retarding the cloud growth[11-18].

2. Types of Security Controls

Security remained the critical issue from long time; however security challenges have increased with the emergence and growth of internet. Whenever, security breach occurs, it results in certain level of compromise. To overcome the security vulnerabilities, various measures that are put in place falls under the following categories: i. Deterrent ii Preventive iii. Detective iv. Corrective *Deterrent:* Deterrent methods make the security harder to breach. In deterrent method, stringent procedures are put in place in order to avoid exploiting the security vulnerabilities. However, deterrent methods do not avoid the security breach altogether, only minimize it. Various methods have been employed and acting as deterrent, for instance, not carrying and inserting the pen drive into the office's computer is one of such measures.

Preventive methods: In the preventive method, tools to prevent the security threat are put in place, anticipating the various known security attacks may strike the computer or the network. This method patches the security vulnerability already known. It prevents any attempt of malware that are trying to ingress into the system.

Detective methods: Detecting method is confined to discovering any security breach that has taken place. Once the attack is detected, control is handed over to the preventive methods. For any new type of attack, new method is developed and incorporated into already existing tools. Therefore, database of attack is continuously grows.

Corrective methods: Once the new software or application is released, it is not hundred percent safe, despite of regression testing and development. Many bugs

pertaining to security issues are detected at later stage. In order to correct these bugs' patches are released and these vulnerabilities are also fixed in next release of the software.

2.1 Security Measures for Cloud Security

Understanding the gravity of security threats, various measures have already been initiated in order to overcome the security challenges. Each of them is attempting to address or mitigate or avoid the security threats in their own way. However, we are highlighting the security guidelines based on prominent security groups, industry and academia.

2.2 Security Groups and Security Measures

Security groups such as NIST, ENISA, CSA has been formed to identify the security threats in cloud domain and suggest measures to prevent security threat. Out of these groups, CSA is entirely dedicated to cloud security whereas, ENISA, & NIST are focusing in other paradigm of IT as well, in addition to the cloud computing. NIST has published various reports to strengthen the cloud security. To meet the security threats and these reports are widely accepted and referred by the industry and academia.To meet the regulatory compliance, cloud matrix model is suggested by Gartner. This document is offering comprehensive guidance to learn the various security threats and regulatory compliance applicable to a specific model and measures to be initiated in order to overcome the specified security threat. Similarly ENISA has published various documents related to security. These documents are widely popular in cloud security domain and referred to learn the security threat.

Cloud security alliance (CSA) is the dedicated group that deals with the cloud security. Unlike other security groups, it is not dealing with other IT issues, instead completely dedicated for cloud security. CSA has published various documents pertaining to cloud security, among them [7-8] are widely popular and can be accessed from CSA website. In addition, CSA is also organizing various workshops and conferences to spread the awareness related to cloud security.Various standards and bodies discussed so far are general in nature; as a result they are not meeting the cloud security in depth. A new model with the nomenclature of FedRAMP has been designed to meet the cloud specific issues such as no control of data, location of database, physical security of cloud resources. FedRamp is gaining a lot of popularity in cloud domain and emerging as a prominent standard for cloud security.

2.3 Academia

Several institution and University are focusing on cloud security. Accordingly, several papers in academia are focused on exploring the security issues in cloud paradigm. Once we review these works, we figure out that majority of Elsevier publications remained restricted to review article only. If we review the IEEE and Springer, we have figure out that the major work in these journals remain concentrated to encryption methods for the improvement of security during data transmission.

Virtualization security is the other area where IEEE papers remained concentrated. For instance [35, 36] are highlighting the virtualization security due to the VLAN network and mapping of VLAN network to the physical resources. Issues related to mapping with the physical resources were also extensively covered.

Study on virtualization security is carried out to identify the security vulnerabilities. They have carried out the cross channel attack, and demonstrated that how a logically separated compartment can easily be accessed with the help of hook and data of other users can easily be accessed or damaged.

3. Industry based solutions for cloud security

Identifying the tremendous business opportunity in cloud security domain, industry is offering wide variety of solutions to meet the security requirement. These solutions can be categorized as described as follows:

- End to end solution
- Server side solution
- Storage solution

Gravity of cloud threat can be determined by reviewing that to avert the risk, either users are not subscribing to the cloud or have deferred switching to the cloud paradigm. Many of them are not subscribing in cases where sensitive information is involved.

Major solutions offered by the industry have been discussed hereunder.

Thales e-security Solution: This is offering wide range of security solutions. All these solutions offered are relying on cryptography to protect the data in shared environment. According to Thales e-security solution, cryptography is old and existing from many years. At the same time proved to be promising relative to the other methods. It can be well applied in the paradigm like cloud that is in the early phase of its evolution. Various solutions offered by Thales e-security are controlling fraud and protecting intellectual property, Data breach notification, trust and identity management.

Cipherworld: Cipherworld is well known organization dealing with the cloud security threat. Cipherworld solutions are primarily driven by internal threat, correspondingly, have suggested tokenization as the method for securing the data. Application of tokenization transform the legitimate text into non-legitimate text, thereby safeguards the data from internal threat.

Tokenization method has been proved to be better method for securing the data relative to the encryption method.

VMware: VMware the leading virtualization solution provider is offering cloud solutions pertaining to virtualization technology. According to VMware, organizations are using the legacy based security tool to secure the cloud, whereas cloud is utilizing the virtualization in great deal. In order to meet the virtualization security need, VMware is offering vCloud and vRealize. Cloud secured in this way is compliant ready cloud; correspondingly, various reports pertaining to compliance can easily be generated.

4. Conclusion

Cloud security is a critical issue and retarding the exponential rate of cloud growth. Various solutions are already suggested by the academia, industry, and security groups to deal with the security threat. However, measures initiated are not enough and additional methods need to be employed to further strengthen the cloud security and compliances. This will be possible only by undergoing the current solution offered by academia and industry. Solution developed after reviewing the current development and identifying the gaps in them will be much more efficient and effective. On one hand these measures will further able to restore the users trust in cloud computing on the other hand will further boost the cloud growth.

References

[1] Barton, M. (2012). Cloud Downtime's Cost: $70m Since 2007, Give Or Take. Retrieved October 29,2012, From Http://Www.Wired.Com/Insights/Author/Mikeburton.

[2] Singh, H. P., Bhisikar, A. & Singh, J. 'Innovative ICT through Cloud Computing', Iup Journal Of Computer Sciences 7(1), 37, 2013.

[3] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J. & Brandic, I. 'Cloud Computing And Emerging It Platforms: Vision, Hype, And Reality for Delivering Computing As The 5th Utility', Future Generation Computer Systems 25(6), 599–616,2009.

[4] Bigo, D., Boulet, G., Bowden, C., Carrera, S., Jeandesboz, J, And Scherrer, A.(2012). Fighting Cyber Crime And Protecting Privacy In The Cloud. Directorate General For Internal Policies Policy Department C: Citizens' Rights And Constitutional Affairs. Available at Http://Www.Europarl.Europa.Eu/Regdata/Etudes/Etudes/Join/2012/462509/Ipol-Libe_Et(2012)462509_En.Pdf.

[5] Coleman, C. (2012, September 25). Cloud Conversion Saves Gsa Millions. Retrieved From Http://Gsablogs.Gsa.Gov/Gsablog/2012/09/25/Cloud-Conversion-Saves-Gsa-Millions/.

[6] Csa (2010). Top Ten Threats In Cloud Computing. Cloud Security Alliance, 2010.

[7] Csa (2013). The Notorious Nine: Cloud Computing Top Threats In 2013. Cloud Security Alliance, 2013.

[8] Cisco. " Forecast And Methodology, 2013–2018." Cisco Global Cloud Index:, 2014.

[9] Gartner (2013).Forecast Overview: Public Cloud Services, Worldwide, 2011-2016, 4q1. Published: 8 February 2013.

[10] Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M. & Pourzandi, M. (2012), 'A Quantitative Analysis of Current Security Concerns And Solutions For Cloud Computing', Journal Of Cloud Computing **1**(1), 1–18.

[11] Gite, V. (2008). Explain: Five Nines (99.999%) Computer / Network Uptime Concept. Available at Http://Www.Cyberciti.Biz /Faq/Computer-Networkuptime-Five-Nines-999999/

[12] Hooper, Christopher And Martini, Ben And Choo, Kim-Kwang Raymond. Cloud Computing And Its Implications For Cybercrime Investigations In Australia (October 15, 2013), Computer Law And Security Review 29(2): 152-163, 2013.

[13] Http://Aws.Amazon.Com/Blogs/Aws/Aws-Data-Transfer-Price-Reduction/

[14] Http://Googlecloudplatform.Blogspot.In/2014/10/Announcing-Across-The-Board-Price-Cuts-On-Compute-Engine.Html

[15] Http://Iwgr.Org.

[16] Janakirammsv(2014), "Cloudtracker, Fourth-Quarter 2014", Technical Report, Gigaom Research, Jan 2015.

[17] Joshi, J. B. D., Bhatti, R., Bertino, E., & Ghafoor, A. (2004). An Access Control Language For Multi-Domain Environments. Ieee Internet Computing, 8(6), 40–50. Doi:10.1109/Mic.2004.53

[18] Kwang, K., Choo, R.(2013).Trends & Issues In Crime And Criminal Justice. Australian Institute Of Criminology, No. 400 October 2010.

[19] Lin, G., Fu, D., Zhu, J., & Dasmalchi, G. Cloud Computing: It As A Service [Ieee]. It Professional, 11(2), 10–13. Doi:10.1109/Mitp.2009.22,2009.

[20] Liu, Y., Sun, Y. L., Ryoo, J., Rizvi, S. & Vasilakos, A. V. 'A Survey Of Security And Privacy Challenges In Cloud Computing: Solutions And Future Directions', Journal Of Computing Science And Engineering **9**(3), 119–133,2015.

[21] Mell, P., & Grance, T. The Nist Definition Of Cloud Computing. Special Publication 800-145, National Institute Of Standards And Technology.Available, 2011. At Http://Csrc.Nist.Gov/Publications/Pubssps.Html#800-145.

[22] Microsoft (2013). Small And Midsize Business Cloud Trust Study. Us Study Result, Jun 2013.

[23] Mualla, K. & Jenkins, D. 'Evaluating Cloud Computing Challenges For Non-Expert Decision-Makers', Ijdiwc P. 285,2015.

[24] Singh, J And Kumar, V (2013).Implementation Of User-End Broker Policy To Improve The Reliability Of Cloud Services. International Journal Of Cloud Applications And Computing, 3(4), 13-27, October-December 2013.

[25] Cisco. " Forecast And Methodology, 2013–2018." Cisco Global Cloud Index:, 2014.

[26] Singh, Jitendra. Cloud Computing For Beginner To Researcher. New York: Cs An Amazon Company, 2014.

[27] Singh, Jitendra. "Comprehensive Solution To Mitigate The Cyber-Attacks In Cloud Computing ." International Journal Of Cyber-Security And Digital Forensics (Ijcsdf), , Vol. 3, Issue 2, Pp. 84-92, 2014.

[28] Singh, Jitendra. "Study On The Response Time In Cloud Computing ." International Journal Of Information Engineering And Electronic Business, , Vol. 5, 36-43, 2014

[29] Singh, Jitendra, And Vikas Kumar. "Assessment Of Security Risk In Cloud Computing Environment." Asia Pacific Business Review, Vol 7, 180-190, 2011.

[30] Singh, Jitendra, And Vikas Kumar. "Multi-Disciplinary Research Issues In Cloud Computing ." Journal Of Information Technology And Research, Vol 7, No. 3, Pp. 32-53, 2014.

[31] Wilcox, J. (2011). Gartner: Most Cios Have Their Head In The Cloud. Retrieved From Http://Betanews.Com/2011/01/24/ Gartner-Most-Cios-Have-Their-Heads-In-Theclouds/.

[32] Yeo, C. S., Buyya, R., Assuncao, M. D., Yu, J.,Sulistio, A., Venugopal, S., & Placek, M. Utility Computing On Global Grids. In H. Bidgoli (Ed.), Handbook Of Computer Networks.Hoboken, 2007.

[33] Oracle(2010),"Strategies For Solving The Datacenter Space,Power, And Cooling Crunch: Sun Server And Storage Optimization Techniques", An Oracle White Paper March 2010.

[34] Hao, Fang, Et Al. "Secure Cloud Computing With A Virtualized Network Infrastructure." Hotcloud. 2010.

[35] Azodolmolky, S., Wieder, P., & Yahyapour, R. Cloud Computing Networking: Challenges And Opportunities For Innovations. Ieee Communications Magazine, 51(7), 54-62, 2013.

Jitendra Singh has completed his masters in computer science from Madurai Kamaraj University and 'C' Level (M. Tech) from National Institute of Electronics and Information technology (NIELIT) India. Master is followed by PhD (Computer Science) in the area of cloud computing. He has also qualified the prestigious UGC-NET examination conducted by the UGC of India in the year 2006.

He has over 13 years of teaching experience during which he has taught to the students of Bachelor and Master Level. He is also engaged with the Stratford University, USA, India Campus, as a part time faculty from over five years. He has contributed around 20 articles in leading refereed journals.

Kamlesh kumar Raghuvanshi has completed his masters in computer Application (MCA)from Jiwaji University Gwalior (MP) , Worked 8+ yrs in IT Industry including company like IBM, TCS, Wipro, Tech-Mahindra and Currently teaching as Assistant professor in Ramanujan College University Delhi Since 2015 He has also qualified the prestigious UGC-NET examination conducted by the UGC of India in the year 2012.