IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Issue-10 E-ISSN: 2347-2693

Is Cloud Secure?

B Balamurugan[1], K Marimuthu[2,*], S Rajkumar[3], Mamdouh Alenezi[4] and R Niranchana[5]

[1]School of Information Technology and Engineering, VIT University, Vellore-632014, India
[2, 3, 5] School of Computer Science and Engineering, VIT University, Vellore-632014, India
[4]Information & Technology Office, Prince Sultan University, Riyadh, KSA

Available online at: www.ijcseonline.org

Received:15/Sep/2016 Revised: 26/Sep/2016 Accepted: 13/Oct/2016 Published: 31/Oct/2016

***Abstract*—Cloud computing is the buzz word, the corporate world pronounces every now and then. All the software companies are looking for a where about to store their data at a low cost and reduce the problem of selecting and updating a suitable infrastructure. The mushroom growth of startups and their prosperity and share in the software trends has also mounted the need of cloud computing. On the other hand, several other problems have taken birth like the believability of the cloud and the security concerns of it [1].The cloud users are stranded in a situation either to believe cloud or to wait for some more time for transiting to cloud .This position paper gives a thorough analysis of the cloud security and the stand the cloud computing has taken currently.**

Keywords- Cloud security alliance; Data loss; denial of service attack; Server Reboot

I. INTRODUCTION

Cloud security research started to grow after several premier cloud service providers provided facts about the attacks and vulnerabilities and the ways to defend it. The security vulnerabilities were also found between competitors storing data with a same cloud service provider. Cloud security alliance (CSC) which promotes the use of best practices for providing security assurance through Cloud Computing [2] has listed quite a lot of attacks that are major threat to cloud computing security [3]. It has also listed the ways to defend the attacks and the architecture to follow for avoiding it. Accordingly, Google had non-transparent security issues leading to breakdown of its service almost nine times, since its inception, followed by amazon and Microsoft having their share of eight and seven times respectively. The case further worsens with small cloud players [4].

II. TREATS AND VULNERABILITIES

Another report by Cloud security alliance (CSC) by reviewing 11,491 news reports articles on cloud computing-security flaws[21-31] from different news sources from 2008 to 2012, says that cloud vulnerability incidents are increasing exponentially every year and there is a huge gap between the growth of security measures and attacks. The Fig. 1 shows the growth of cloud outrages upon time. The CSA top treat list is on an increasing spear and the cloud service providers are more concerned about deploying cloud services faster and cutting down costs [8] to lure more customers [6].Of the treats that are uncontainable, the Insecure Interfaces and API's leads the race forming majoring treat followed by Data Loss and Leakage [5].The cloud providers are judged by their response time, availability and security for a prolonged time frame. For analysing the end-user experience of the paas and laas cloud providers from around the world, the Global Provider View [7] monitors continuously an application hosted and running in all the top cloud computing service providers of the world and feeds the live status about how well they perform over time. The status shows that the availability of the cloud service providers is 100% only for about 10 service providers out of 150 of them and response time is good for only half of them. Considering the non-availability factor as a breakdown due to unreasoned security concerns or an DOS (denial of service) attack, it establishes that security factor is overall in a weak position to store vital information like health and finance data.

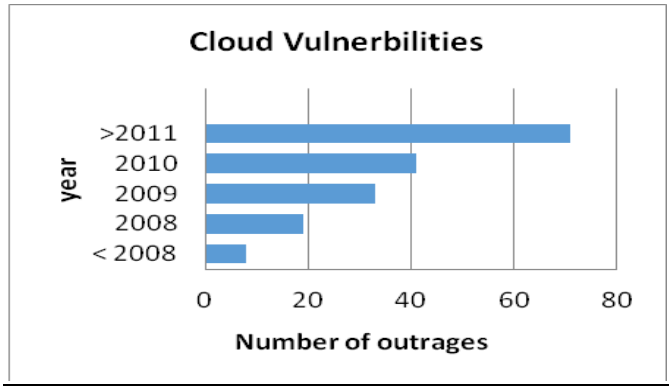

Fig. 1. Cloud vulnerabilities

*Corresponding Author:
K.Marimuthu
e-mail: k.marimuthu@vit.ac.in , Tel.: +91-8526006159

III. RECOVERY FROM ATTACKS

Considering the recovery time, after a breakup of service, it takes at least 21 days to get back to normal after a failure [9] and if it involves hardware failures and natural disastrous one, it takes an additional time. The possibility of reoccurring from a failure is of deprived probability and it's dreadful for companies that have critical applications on the cloud. Compuware[9] ,a company particularly specialist in measuring the Business Impact of Technology Performance has stated that the loss due to non-availability of cloud is about $782,600 together for all global cloud service vendor per year [10].

There is another significant factor for examining the Quality of service (QOS) of the cloud provider with respect to availability. Cloud performance analyser, an application [11] analyses the key response time of an application loaded in amazon EC2-east and its availability over different geographical locations and examines the response time factor with distance factor. The application shows average response time greater than 16 minutes in most regions, considered only to be a substandard response time.

Initially software companies' stored data that are not crucial like deposits, in cloud to cut costs, currently companies are looking at storing primary vital information like monetary data and health data over the cloud. Cloud security has also increased the possibility of a company to co-work with its vendors over cloud, nullifying the difference of their architecture and environment. Cloud architectural change is done in all possible ways to sustain the security makeover that are needed to keep cloud safe. Even then, on the other side, the vulnerabilities are also on increase, making cloud non suitable for very secure process and storage.

The cloud service provider's view of customers to secure the own data has vanished ,as cloud users compare cloud service providers with the view of security provided and has the option of selecting the one with maximum security potential and less history of attacks. Fig. 2 explains the reason for a customer using a cloud service and very less of them use it for security reasons. The customer evaluates a cloud provider with the help of the standards they follow in terms of security .Organizations like NIST, IEEE and ENISA had come out with different strategies to be followed by cloud providers and even updates the standards regularity. The standard organizations has also the power to audit the cloud service provider, on timely basis about it compelling with the specification .The cloud service providers ,most of the time follow the standards initially at the time of deployment and they slowly lose grip. For example, SP 800-144 is geared toward system managers, executives and information officers making decisions about cloud computing initiatives and it is impossible for these people to take decision according to the template as it is not feasible during implementation, tending to reduce security eventually [12].This regulatory risks will lead to breach of security and privacy as well as legal issues.

Taking in to account, the Service Level Agreement (SLA) as a prerequisite for a matured agreement of superior security to be provided by Cloud service providers to the cloud users is the basis for managing and coordinating services [15]. SLA is a written agreement about service levels offered by providers to customers [16].Example of these SLA include a the Go Grid SLA [5].A traditional SLA covers the elements of the Service like Server Uptime, Persistent Storage, Network Performance, on time Load Balancing, Cloud Storage, Server Reboot, Support Response Time, Domain Name Services and Physical Security. Considering all the factors into account, most of them deal with performance and availability of the cloud service over the security of the cloud. This thoroughly states that the SLA is not a big exercise for achieving secure cloud service. These issues hinder organizations from adopting cloud service, but still cloud providers are not addressing the problems [13] [14].

Lot of research is on cloud security metrics, as traditional security metrics can't be applied for cloud computing. The exercises of metrics are classified into strategic support, quality assurance and tactical oversight [17] [18]. NIST follows three types of metrics [19-30]. While validating the metrics that are available as a standard for cloud service providers, it is sad to find that most of the attributes are dealing with hosting the cloud, availability and not much on security. The metrics framework lacks security attributes. When the data by the client is stored with the cloud provider or the processor who is the sub-contractor and is accessed by the client or the processor in a SaaS (software as a service) pattern, security breach will lead to dismay to the client more than to the cloud provider, as the former vital data or service is not available for the point in time. The cloud provider with the help of his guiding principle will have a safe lead, on the other hand ,the cloud user have to worry about the status of data tomorrow and the recovery process time.

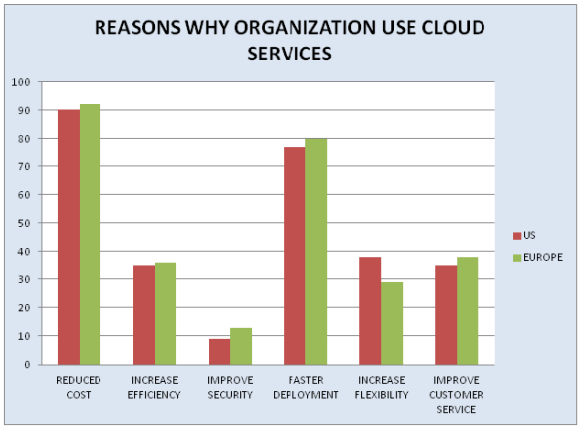

Fig.2. Reasons for organisation using cloud

The physical location of the data should also be considered as a factor [20], as in several cases the location will be in an area with lot of natural calamities and weather severity leading to dismay. The knowledge of physical location of a public cloud is almost nil to the user when compared to that of private cloud users .The cloud essentials of the environment, like as VMs, hypervisors, virtual network devices, might be regularly relocated for load-balancing strategy. In the current scenario there is no assurance for the client about the physical security applied across all potential locations. There are several approved countries like EU/EEA for cloud storage and permission are available for a cloud provider to shift inside the continent, the cloud data servers, but no strategy is available for the users to know the physical location. The client /server data communication is monitored using a continuous monitoring system to reduce attacks and treats, cloud must also have real-time service level feeds including service level dashboards, enabling the cloud user to know live status of their data. Regular service level reports can be provided to enhance believability. None of the current cloud service provider communicates incident reports and alerts the cloud user, forecasting the devastations. APIs can be installed in users system to live feed the status of their data.

The cloud providers have to simulate and test different scenarios to improve adaptability .Cloud providers doesn't do this as it incurs extra costs for them per deployment. Penetration tests, Backup/failover tests and Data portability tests are to be done on a timely basis. Availability has to be measured and drills has to be conducted for data availability .Scheduled unavailability has to prepared, finding out the time with less client activity. This will lead the cloud providers to raise the flag when needed.

When an incident happens, the cloud providers don't analyse and classify it, leading it to occur again. Things like, what is the relentless incident, how many such incidents have occurred and how swiftly did the provider respond, how quickly it was detected have to be questioned and analysed. Evaluation techniques are not available in abundant with the cloud providers to assess the security and categorize the cloud providers security .Classifying the providers to category will give a lot of suggestion to the user before choosing a service provider and the same will also increase the growth of newer security protocols and standards. A internet and mobile service provider are categorised in such a manner to increase fresh competition leading to advantage for the uses. Benchmarking their process of deployment and security to a standard is not available in the current state of affairs and should be brought up. Benchmark score should be displayed and listed for the respective cloud providers by a forum like cloud security alliance.

IV. CONCLUSION

As a conclusion of the hypothesis, whether cloud computing is safe or not for storage and computing. The answer may be it lacks in certain areas of security, being reflected in the failing, that are occurring as vulnerability. If the cloud security is not taped, measured and optimized, it might limit the growth of cloud in coming days.

REFERENCES

[1] R. K. L. Ko, "Cloud computing in plain English," ACM Crossroads, vol. 16 (3), pp. 5-6, 2010.

[2] https://cloudsecurityalliance.org

[3] https://cloudsecurityalliance.org/research/vulnerabilities

[4] https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview

[5] https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[6] http://www.symantec.com/connect/blogs/avoiding-hidden-costs-cloud-0, Created: 15 Jan 2013, Updated: 15 Jan 2013 ,Tom Powledge.

[7] https://cloudsleuth.net/global-provider-view

[8] Shu-Min Chuang; Kuo-En Chang; Yao-Ting Sung, "The cost effective structure for designing hybrid cloud based enterprise E-learning platform," Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on , vol., no., pp.523,525, 15-17 Sept. 2011

[9] http://www.compuware.com

[10] http://www.compuware.com/en_us/about/techfail.html

[11] https://cloudsleuth.net/cdn-performance-analyzer

[12] https://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

[13] Shaheen Ayyub and Devshree Roy, "Cloud Computing Characteristics and Security Issues", International Journal of Computer Sciences and Engineering, Volume-01, Issue-04, Page No (18-22), Dec -2013,

[14] Reddy, Varun K., and Jagadeeshwar E. Rao. "A Survey on Security in Cloud Using Homographic and Disk Encryption Methods." International Journal of Computer Sciences and Engineering 2 (2014).

[15] Putri, N.R., Mganga, M.C. 2011. Enhancing Information Security in Cloud qe Computing Services using SLA Based Metrics. Master's thesis: Blekinge Institute of Technology.[Online].

[16] Mewada, Shivlal, Umesh Kumar Singh, and Pradeep Sharma. "Security Based Model for Cloud Computing." Int. Journal of Computer Networks and Wireless Communications (IJCNWC) 1.1 (2011): 13-19.

[17] Mewada, Shivlal, Umesh Kumar Singh, and Pradeep Sharma. "Security Enhancement in Cloud Computing (CC)." International Journal of Scientific Research in Computer Science and Engineering 1.01 (2013): 31-37.

[18] K. Erkan, "Evaluating IT Security Performance with Quantifiable Metrics", Institutionen f¨or Data- och Systemvetenskap, KTH.

[19] E. Chew, M. Swanson, K. Stine et al., "Performance Measurement Guide forInformation Security," NIST Special Publication 800-55 Revision 1, National Institute of Standards and Technology & U.S. Department of Commerce, 2008.

[20] http://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

[21] Niketan Jivane, Supriya Jivane, S.Rajkumar and K.Marimuthu, "Enhancement of an algorithm to extract text-lines from images for blind and visually impaired persons through parallel approach, International Journal of Computer Sciences and Engineering 4(9), pp. 25-32, 2016.

[22] Xiong Li, Jianwei Niu, Marimuthu Karuppiah, Saru Kumari, Fan Wu(2016), Secure and Efficient Two-factors User Authentication Scheme with User Anonymity for Network Based E-Health Care Applications., Journal of Medical Systems, DOI: 10.1007/s10916-016-0629-8.

[23] Marimuthu Karuppiah, Saru Kumari, Xiong Li, Fan Wu, Muhammad Khurram Khan, R Saravanan, Sayantani Basu,(2016), A Dynamic ID-based Generic Framework for Anonymous Authentication Scheme for Roaming Service in Global Mobility Networks, Wireless Personal Communication, DOI: 10.1007/s11277-016-3672-3.

[24] Saru Kumari, Marimuthu Karuppiah, Xiong Li, Fan Wu, Ashok Kumar Das, Vanga Odelu (2016), A Secure Trust-Extended Authentication Mechanism for VANETs, Security and Communication Networks, DOI: 10.1002/sec.1602.

[25] Marimuthu Karuppiah, Saru Kumari, Ashok Kumar Das, Xiong Li, Fan Wu, Sayantani Basu (2016), A Secure Lightweight Authentication Scheme with User Anonymity for Roaming Service in Ubiquitous Networks, Security and Communication Networks, DOI: 10.1002/sec.1598.

[26] Marimuthu Karuppiah(2016), Remote User Authentication Scheme using Smart card: A Review, International Journal of Internet Protocol Technology, 9(2/3): 107–120.

[27] Fan Wu, Lili Xu, Saru Kumari, Xiong Li, Ashok Kumar Das, Muhammad Khurram Khan, Marimuthu Karuppiah, Renuka Baliyan (2016), A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks, Security and Communication Networks, DOI: 10.1002/sec.1558.

[28] Swapnil Rajesh Telrandhe and Deepak Kapgate, "Authentication Model on Cloud Computing", International Journal of Computer Sciences and Engineering, Volume-02, Issue-10, Page No (33-37), Oct -2014,

[29] S. Mewada, P. Sharma and S. S. Gautam, "Exploration of efficient symmetric algorithms," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2016, pp. 663-666

[30] Karuppiah, Marimuthu, and R. Saravanan. "A secure remote user mutual authentication scheme using smart cards." Journal of information security and applications 19.4 (2014): 282-294. -

Authors Profile

B. Balamuruaan works its Associate Professor in School of Information Technology and Engineering ,VIT University,Vellore campus.He completed his B.E computer science and Engineering from Bharathidasan university and M.E computer Science under Anna University. He has published more than 80 research papers in reputed international conferences and journals His potential area of interests includes cloud computing and big data.

K. Marimuthu received his B.E. degree in Computer Science & Engineering from Madurai Kamaraj University, Madurai, India in 2003, M.E. degree in Computer Science & Engineering from Anna University, Chennai, India in 2005 and PhD degree in Computer Science & Engineering from VIT University, Vellore, India in 2015. He is now an Associate professor in School of Computing Science & Engineering, VIT University, Vellore, India. He has published more than 25 research papers in reputed international conferences and journals. He is a life member of Cryptology Research Society of India (CRSI). His main research interests include cryptography and wireless network security, in particular, authentication and encryption schemes.

S. Rajkumar is currently working as an Assistant professor (Senior) in Department of Computer Science and Engineering, VIT University, Vellore, India. He received his B.E degree in Computer Science and Engineering from Anna University, Chennai, India in 2008, M.E degree in Computer Science and Engineering from Anna University, Chennai, India in 2010. He is pursuing his PhD at VIT University, Vellore, India. He has submitted his Ph.D. Thesis on August 2016. His research interest includes Digital image processing, Computer Vision, Visual Perception, Object detection, Medical image processing and Infrared image processing. He has published several refereed research papers in various reputed international conferences and journals. He is a reviewer for many reputed journals like Computer Biology and Medicine, Journal of Medical Imaging and Health Informatics etc. He is a life member of CSI.

Mamdouh Alenezi received his B.S. degree in Computer Science from Prince Sultan University, Riyadh, KSA in 2010, M.S. degree in Software Engineering from DePaul University, Chicago, IL, USA in 2011 and PhD degree in Software Engineering from North Dakota State University, ND, USA in 2014. He is now Chief information and Technology officer in Prince Sultan University, Riyadh, KSA. He has published more than 25 research papers in reputed international conferences and journals. His main research interests include software engineering.

R Niranchana received her B.E degree in Computer Science and Engineering from Anna University, Chennai, India in 2005, M.E degree in Computer Science and Engineering from Anna University, Chennai, India in 2008. She is pursuing his PhD at VIT University, Vellore, India. Her main research interests include cryptography and wireless network security, in particular, authentication and encryption schemes.

