Volume 3, Issue 8, August 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Multi-Cloud Architecture to Reduce Security Risks in Cloud Computing

Vinod Kumar Paidi*, P.Varaprasada Rao
Department of CSE & JNTUH
India

Abstract- Cloud computing has emerged as a new model of computing. It is a paradigm shift in computing history. Cloud services can be availed without capital investment as they are commoditized. Cloud users get services in pay per use fashion and enjoy many benefits of cloud including low cost and accessibility from anywhere in the world. However, users have security concerns as they outsource their valuable business data to cloud and treat the cloud as "untrusted". With a single cloud service provider there might be the risk of service availability, failure possibility and insider theft of data. Moving towards multiple clouds can address security problems. This paper aims of investigating how multi-cloud deployments can reduce security risk and have impact on the usage of the cloud computing technology. We built a prototype application to simulate the advantages of using multi-clouds to improve security. The empirical results revealed that multi-clouds can reduce security risks.

Index Terms – Cloud computing, security, single cloud, multi-clouds

I. Introduction

Cloud computing is being used by many organizations and the benefits are realized by general public in many ways. Cloud service providers such as IBM, Microsoft, Amazon, Oracle and so on are providing various kinds of cloud services. The services include Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS). These services can be used by cloud users in pay per use fashion without investment. According to Subashini and Kavitha [1], cloud computing can be used by small and medium sized companies to increase their potential to serve their clients better and generate more revenues by reducing the existing infrastructure costs. However, for rapid growth of cloud computing, the cloud providers are supposed address security issues in cloud storage with high priority. It has been observed that single cloud usage has problems in service availability, failure rate, and insider theft and so on. For this reason there was considerable research into the study of multi-cloud usage for curbing security problems. This paper provides necessary insights into the usage of multi-clouds and the possible reduction in security risk of cloud data storage. Cloud users expect protection to their confidential information which has been outsourced to client. The data might include sensitive personal information, health related records which is critical and to be protected from malicious insider attacks.

This paper throws light into various cloud features, deployments, service models, single cloud, and multi-clouds from security perspective. The remainder of this paper is structured as follows. Section II provides review of literature. Section III provides security risks in cloud computing. Section IV describes proposed security architecture. Section V provides the proposed prototype to simulate the benefits of using multi-clouds. Section VI presents experimental results while section VII concludes the paper.

II. PRIOR WORK

This section provides brief summary review of prior works on cloud computing with respect to security. Multi-shares with secret sharing algorithm was proposed in [2] for cloud security and data integrity. In [3] cloud security was explored using cryptographic methods. The security risks addressed include service availability, data intrusion, and data integrity. The solution used cloud storage and multi-clouds. In [4] a survey has been made to know security issues and solutions with respect to single cloud. In [5] RACS and RAID kind of techniques were used for cloud security using multi-clouds. In [6] client centric distributed protocols were explored for data integrity with multi-clouds usage. In [7] service availability problem was focused in single cloud environment. In [8] there was discussion about cloud security issues. In [9] cryptography is used to protect cloud data in single cloud environment. In [10] a security mechanism by name "Depot" is used to single cloud environment. A security mechanism by name "Venus" was proposed in [11] which focused on data integrity issue in single cloud environment. Service availability was focused in [1] in single cloud environment. In [12] a survey is made on cloud security. In [13] cloud data integrity is focused in single cloud environment. In [14] a new security mechanism was proposed by name "HAIL" for improving service availability in multi-cloud environment. In [15] a survey was done on cloud data integrity in multi-cloud environment. Encrypted cloud VPN technique is used in [16] for data integrity in multi-cloud environment. Cloud security was discussed in [17] in single cloud environment. TCCP techniques for cloud data integrity issues and service availability were presented in [18] in single cloud environment. Homomorphic tokens and erasure codes were used in [19] to ensure cloud data integrity in single cloud environment. PDP schemes were used to protect data integrity in clouds. In [20] cloud computing security was explored in single cloud environment.

III. SECURITY RISKS IN CLOUD COMPUTING

There are three important security risks identified in cloud computing. They are data integrity, data intrusion and service availability. Data integrity is the one that causes most of the security problems. This is because the data is very vulnerable to cloud users. Loss of data integrity has severe impact on them. Many researches were found on this security risk [15], [21], [22] and [23]. Data intrusion is another security risk which is possible when hackers gain access to sensitive information. To address such problem considerable research was carried out [24], [20]. Service availability is another security risk which is very important from client point of view. Cloud clients expect round the clock availability of cloud services. Many service availability risks were explored in [25], [15], [20], and [26].

IV. PROPOSED ARCHITECTURE

In this paper we propose an architecture for multi-cloud which is similar to the one presented in [8]. The architecture has provision for multiple clouds that work together. It can be called as cloud of clouds. The architecture is as shown in fig. 1.

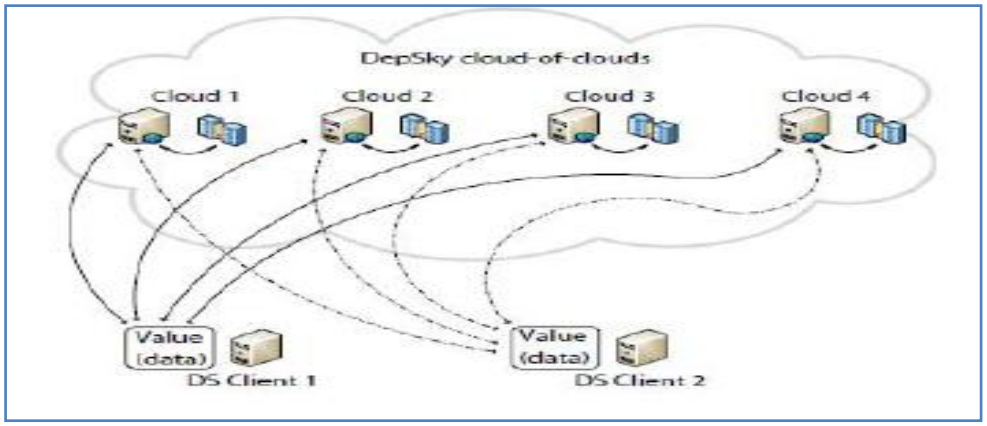

Fig. 1 – Multi-cloud architecture (excerpt from [3])

As can be seen in fig. 1, it is evident that the architecture has provision for multiple clouds. The data outsourced by clients can store in any cloud. It does mean that the multiple clouds work together. This will automatically improve service availability and reduce the risk of losing data as well. With regard to internal theft strict measures are to be used by cloud service providers.

V. PROTOTYPE APPLICATION

We have built a prototype application in distributed environment. The application demonstrates the presence of multiple clouds and their storage dynamics. The application is built in Java platform to simulate the multi-cloud environment. The environment used for application development is a PC with 4 GB RAM, Core 2 dual processor running Windows 7 operating system. Net Beans is the IDE used for development. The server programs were built in such a way that they work together to reduce security risk.

VI. EXPERIMENTAL RESULTS

From the experiments on multiple clouds it has been observed that, the storage security risk is considerably reduced when number of clouds is increased. The simulation results revealed this fact.

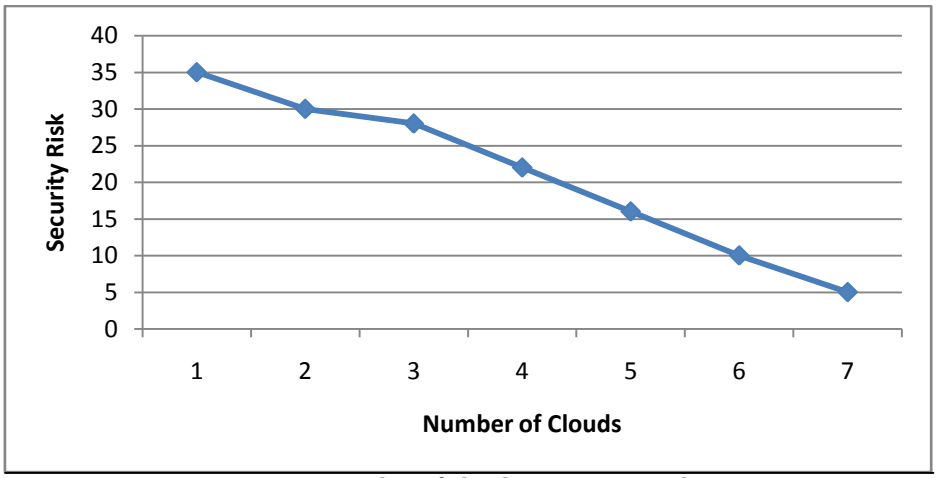

Fig. 2 – Number of clouds vs. security risk

As can be seen in fig. 2, it is evident that the horizontal axis represents number of clouds while the vertical axis represents security risk. The results reveal that the security risk is reduced when number of clouds is increased.

August - 2013, pp. 1150-1152

VII. Conclusion

Cloud computing phenomenon is rapidly growing. Cloud users are able to get services with low cost and greater accessibility. However, their security concerns are to be addressed. In this paper, we proposed an architecture that makes use of multiple clouds together to improve service availability and reducing the risk of data loss. We have implemented a custom Java simulator application that demonstrated the usefulness of multi cloud. The experimental results revealed that the multiple clouds are capable of reducing security risk.

References

[1] S. Subashini and V. Kavitha, "A survey on securityissues in service delivery models of cloudcomputing", Journal of Network and ComputerApplications, 34(1), 2011, pp 1-11.

[2] M.A. AlZain and E. Pardede, "Using Multi Sharesfor Ensuring Privacy in Database-as-a-Service",44th Hawaii Intl. Conf. on System Sciences(HICSS), 2011, pp. 1-9.

[3] A. Bessani, M. Correia, B. Quaresma, F. André andP. Sousa, "DepSky: dependable and secure storagein a cloud-of-clouds", EuroSys'11:Proc. 6thConf. OnComputer systems, 2011, pp. 31-46.

[4] F. Rocha and M. Correia, "Lucy in the Sky withoutDiamonds: Stealing Confidential Data in theCloud", Proc. 1stIntl. Workshop of Dependabilityof Clouds, Data Centers and Virtual ComputingEnvironments, 2011, pp. 1-6.

[5] H. Abu-Libdeh, L. Princehouse and H.Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium onCloud computing, 2010, pp. 229-240.

[6] C. Cachin, R. Haas and M. Vukolic, "Dependablestorage in the Intercloud", Research Report RZ,3783, 2010.

[7] A.J. Feldman, W.P. Zeller, M.J. Freedman andE.W. Felten, "SPORC: Group collaboration usinguntrusted cloud resources", OSDI, October2010, pp. 1-14.

[8] E. Grosse, J. Howie, J. Ransome, J. Reavis and S.Schmidt, "Cloud computing roundtable", IEEESecurity & Privacy, 8(6), 2010, pp. 17-23.

[9] S. Kamara and K. Lauter, "Cryptographic cloudstorage", FC'10: Proc. 14thIntl.Conf. on Financialcryptograpy and data security,2010, pp. 136-149.

[10] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi,M. Dahlin and M. Walfish, "Depot: Cloud storagewith minimal trust", OSDI'10: Proc. of the 9thUSENIX Conf. on Operating systems design andimplementation, 2010, pp. 1-16.

[11] A. Shraer, C. Cachin, A. Cidon, I. Keidar, Y.Michalevsky and D. Shaket, "Venus: Verificationfor untrusted cloud storage", CCSW'10: Proc.ACM workshop on Cloud computing securityworkshop, 2010, pp. 19-30.

[12] H. Takabi, J.B.D. Joshi and G.-J. Ahn, "Securityand Privacy Challenges in Cloud ComputingEnvironments", IEEE Security & Privacy, 8(6), 2010, pp. 24-31.

[13] M. Van Dijk and A. Juels, "On the impossibility ofcryptography alone for privacy-preserving cloudcomputing", HotSec'10: Proc. 5thUSENIX Conf. onHot topics in security, 2010, pp.1-8.

[14] K.D. Bowers, A. Juels and A. Oprea, "HAIL: Ahigh-availability and integrity layer for cloudstorage", CCS'09: Proc. 16th ACM Conf. onComputer and communications security, 2009, pp.187-198.

[15] C. Cachin, I. Keidar and A. Shraer, "Trusting thecloud", ACM SIGACT News, 40, 2009, pp. 81-86.

[16] Clavister, "Security in the cloud", Clavister WhitePaper, 2008.

[17] T. Ristenpart, E. Tromer, H. Shacham and S.Savage, "Hey, you, get off of my cloud: exploringinformation leakage in third-party computeclouds", CCS'09: Proc. 16thACM Conf. onComputer and communications security, 2009, pp.199-212.

[18] N. Santos, K.P. Gummadi and R. Rodrigues,"Towards trusted cloud computing", USENIXAssociation, 2009, pp. 3-3.

[19] C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuringdata storage security in cloud computing",ARTCOM'10: Proc. Intl. Conf. on Advances inRecent Technologies in Communication andComputing, 2010, pp. 1-9.

[20] S.L. Garfinkel, "An evaluation of amazon's gridcomputing services: EC2, S3, and QS", TechnicalReport TR-08-07, Computer Science Group,Harvard University, Citeseer, 2007, pp. 1-15.

[21] J. Hendricks, G.R. Ganger and M.K. Reiter, "Lowoverheadbyzantine fault-tolerant storage",SOSP'07: Proc. 21st ACM SIGOPS symposium onOperating systems principles, 2007, pp. 73-86.

[22] RedHat, https://rhn.redhat.com/errata/RHSA-2008-0855.html.

[23] Sun, http://blogs.sun.com /gbrunett/entry/ amazon_s3_silent_data_corruption.

[24] S.L. Garfinkel, "Email-based identification andauthentication: An alternative to PKI?", IEEESecurity and Privacy, 1(6), 2003, pp. 20-26.

[25] Amazon, Amazon Web Services. Web serviceslicensing agreement, October3,2006.

[26] H. Krawczyk, M. Bellare and R. Canetti, "HMAC:Keyed-hashing for message authentication",Citeseer, 1997, pp. 1-11.

AUTHORS

Vinod Kumar Paidi is student of GRIET College of Engineering and Technology, Hyderabad, AP, INDIA. He has received B.Tech Degree in Computer Science and Engineering from JNTUK, pursuing M.Tech Degree in Computer Science and Engineering. His main research interest includes Cloud Computing, Databases and DWH.

P.Varaprasada Rao is presently professor in Dept. of Computer Science, GRIET, Hyderabad. He completed Masters Degree in Information Technology from Andhra University in the year 2006. He is currently pursuing the PhD in Data Mining area from JNTUH. In his credit there are 1international conference publications.

