Multi-Cloud Based Framework for Improved Service Availability and Security

L.Naveen Kumar[#1], K.Kiran Reddy[*2]

[#1]M.Tech, Computer Science Engineering, MLRIT, Hyderabad, Andhra Pradesh, India
[#]Associate Professor, Department of CSE, MLRIT, Hyderabad, Andhra Pradesh, India

Abstract--Cloud computing has been recognized by the world as a new model of computing that enables users to access huge computing resources. This has been made possible due to the commoditization of computing resources through cloud computing technology. Users from any corner of the world can avail cloud services without making capital investment. However, they are supposed to pay bills as per the usage. Though the technology brings about plethora of benefits to individuals and organizations, they cause security concerns as well. This is because users are to store their data in untrusted servers believing in the security mechanisms of cloud service providers. With a single provider there is risk of data theft, failure and service availability problems. This problem can be addressed by moving from single to multicloud thus having more options that can reduce risk and improve availability of service. In this paper we built multicloud environment. We develop a custom simulator that demonstrates the proof of concept. The empirical results revealed that the proposed multicloud approach is effective and feasible.

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

I. INTRODUCTION

Cloud computing is the technology that leverages the efficiency of individuals and organizations by enabling them to have instant access to state-of-the-art computing resources in pay per use fashion. There are many cloud service providers as of now. They are Microsoft. Amazon, IBM, Oracle, People Soft and so on. These companies are making cloud business and provide a variety of services. The main service models of cloud are Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS). These services can be available by users based on their needs and pay bills as required. Subashini and Kavitha [1] opined that small and medium organizations can make use of cloud services and get benefits from it to strengthen their business capabilities. By utilizing the infrastructure of the cloud service providers, the organizations across the world can grow faster as the services provided by the cloud are cheaper. Cloud service providers are supposed to provide high security to cloud services in order to attract more users towards cloud. There is an important observation that a single cloud has certain concerns. For instance it may cause failure, insider theft, service availability problems and so on. To overcome this problem there exists research towards moving to multi-cloud environments. In multi-cloud environments, there will be more chances to have 24/7 service availability, security and reduced risk to the stored business data. Cloud users want their data to be kept confidential besides expecting cloud service providers to be foolproof in providing security mechanisms. This is because; the data stored includes sensitive information such as personal health records that is very important for the businesses. Such data has to be protected from insider attacks.

This paper discusses cloud features, security, and service models, single to multi-clouds, deployments and so on. 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 reviews literature that has been available on cloud computing security issues and other related topics. There were many researches that focused on cloud computing security issues. For instance in [2] multi-shares was proposed that makes use of secret sharing algorithm. Cryptographic methods were explored in [3] for protecting cloud services. Many security risks are addressed including data integrity, service availability and data intrusion. This is achieved using multi-clouds. A survey was made as explored in [4] to know the things going on in the industry with respect to cloud computing. The survey focused on security issues and moving towards from single to multi-cloud. RAID and RACS are the techniques used in [5] for securing multi-clouds. Distributed protocols which are client centric are explored in [6]. Such protocols are client centric and provide data integrity in multi-cloud environments. Single cloud environment is sued in [7] to solve service availability problem. Cloud security issues were discussed in [8] and the cryptography is used as security solution in [9] in single cloud contexts.

"Depot" is the security mechanism proposed in [10] in single cloud context. Another security mechanism by name "Venus" is used in [11] for data integrity in the single cloud context. In [1] service availability is focused while in [12] a survey is made on security in the single cloud environment. Another security mechanism by name "HAIL" was introduced in [13] in order to improve service availability. This work is done in multi-cloud environments. A survey was made in [14] in multi-cloud environment with respect to data integrity. In [15] encrypted cloud technique by name VPN is used for data integrity in case of multi-cloud environment. In [16] single cloud environment is used to study the cloud storage security. In [17] TCCP techniques were introduced for cloud data integrity and improve the service availability of cloud. In [18] many security mechanisms were introduced such as erasure codes and homomorphic tokens a for the purpose of data integrity in single cloud context. Many PDP (Provable Data Possession) scheme came into existence for cloud data integrity. In [19] more focus was made on cloud security in single cloud environment.

III. SECURITY RISKS IN CLOUD COMPUTING

Cloud computing environment has many known security risks identified by researchers. The problems include service availability, data intrusion, data integrity and other such risks. Data integrity is the main cause of concern. The reason behind this is that the cloud data storage comprises company's valuable data that has to be protected. Otherwise it simply jeopardizes the interests of cloud users. Data integrity is very important in cloud storage as loss of it has severe impact on businesses. Security risks have been identified by many researchers as explored in [14], [20], [21] and [22]. Another security risk identified with cloud computing domain is data intrusion which is nothing but gaining access to sensitive information illegally. Many solutions came into existence in order to address these issues [23], [19]. Another important security risk in cloud computing is the service availability from users point of view. As client expects more availability and security in cloud services, the service availability and security risks are explored in many researches including [24], [14], [19], and [25].

IV. PROPOSED ARCHITECTURE

Architecture has been proposed for storage security using multiple clouds integrated. The idea is conceived from [3]. Many clouds work together and that phenomenon are known as multi-cloud or cloud of clouds. Figure 1 shows the multi-cloud architecture.

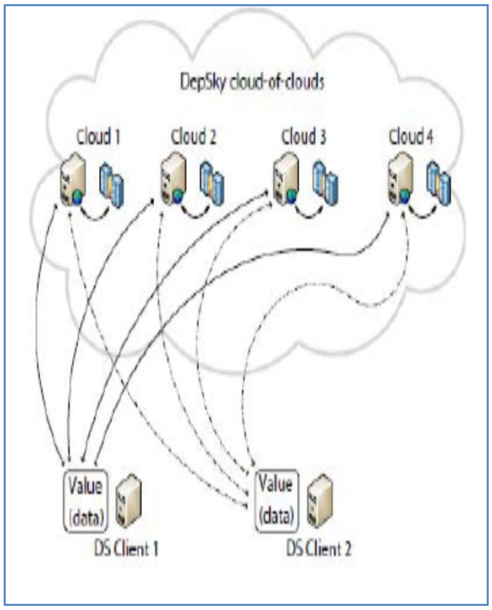
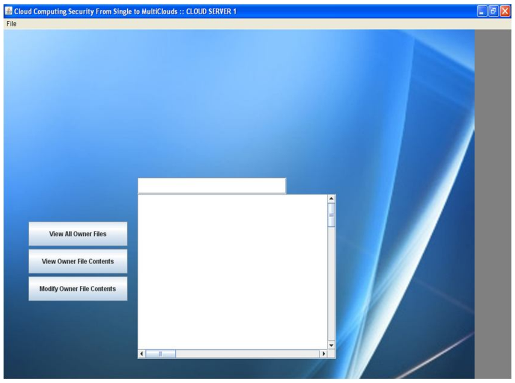


Fig. 1 – Multi-cloud architecture (excerpt from [3])

As seen in figure 1, the architecture has multiple clouds that work together. Many clients interact with the clouds simultaneously. The data is being outsourced by the clouds to multiple clouds. This mechanism improves service availability, reduces the risk of insider theft besides making it more usable and available. The multi-cloud environment has choices that can be utilized by cloud users in order to safeguard their data and also have best services online.

V. PROTOTYPE APPLICATION

We built a custom simulator that demonstrates the proof of concept. The applications simulates the presence of multiple clouds that are connected together to provide best services to cloud users. They are robust in data dynamics and applying required security mechanisms to protect the valuable data of cloud users. 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. A typical cloud service with user interface is as shown in figure 2.



Cloud Computing Security From Single to MultiClouds :: CLOUD SERVER 1
File
View All Owner Files
View Owner File Contents
Modify Owner File Contents

Fig. 2 – Typical cloud server

A typical cloud user interface is as shown in figure 3.

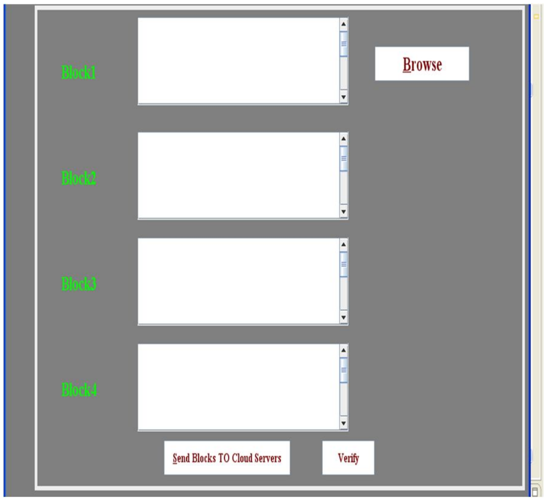


Fig. 2 – typical cloud user interface

This interface allows users to upload files to multiple servers and then get them back securely whenever they need again. In order to receive the data the interface shown in figure 3 is used by cloud users.

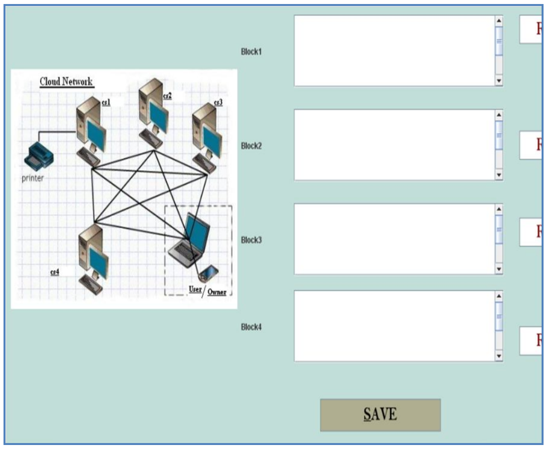


Fig. 3 – Interface to retrieve cloud data

As can be seen in figure 3, the cloud user can use this interface to obtain data securely from multiple clouds. The data is retrieved only after security verifications. The internal theft is not possible and the data availability is enhanced besides reducing the risk of security.

VI. EXPERIMENTAL RESULTS

Experiments are made using multiple clouds being used by many users simultaneously. The observations include that the service availability has been increases besides reducing the risk of insider theft. Storage security has been increased thus making it a feasible solution. The simulation results are presented in the following graphs.

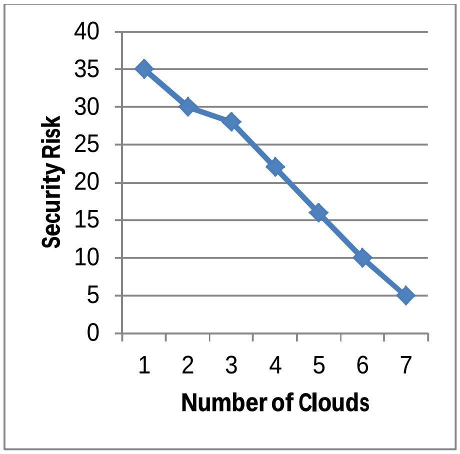


Fig. 4 – Number of clouds vs. security risk

As can be seen in fig. 4, 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.

VII. CONCLUSION

Cloud computing technology has grown to the extent where users can store their business data in cloud storage. Outsourcing such data to cloud has plethora of advantages. But the cloud users have security concerns as the cloud service providers usually do not take care of complete end to end security of cloud data. To address the security concerns of cloud users, in this paper, we implemented a multi-cloud environment where users can store data in multiple clouds. The advantages of this kind of environment include high service availability, low security risks and the insider theft is eliminated to a greater extent.

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] 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.

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

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

[16] 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.

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

[18] 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.

[19] 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.

[20] 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.

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

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

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

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

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