International Journal of Grid and Distributed Computing
Vol. 9, No. 6 (2016), pp.45-50
http://dx.doi.org/10.14257/ijgdc.2016.9.6.05

Review: Ad-Hoc Cloud Architecture & Modern Cryptography

Jitendra Singh Sengar[1] , Richa Sharma[2]

[1]*JSSRLPSP, Gwalior, India*
[2]*ITM University, Gwalior, India*
[1]*jitendrasinghsengar@gmail.com*, [2]*neetu.18sharma12@gmail.com*

Abstract

This paper is showing the review study on cloud architecture that uses donation based resources in a network & helps multiple organizations to collaborate and yet compete with each other. The resources are utilized non intrusively. Organizations collaborate to create a Data-centre, that doesn't harm their existence or profitability. At the same time, these organizations can compete by spreading to those locations where they carry certain edge over theirs. An ad-hoc cloud in heterogeneous environment helps to venture into remote areas. To achieve this some, ad-hoc cloud architecture is proposed along with issues and strategies. This is being elaborated in this paper with some effective sense.

Keywords*: Ad-hoc Cloud, Cloud Computing, Cryptography*

I. Introduction

Cloud computing has data and services reside in common space in elastic data centers, and the services are accessible by authentication. The services are composed using highly elastic and configurable resources. Cloud computing [1] services form a strong service foundation framework to provide any kind of service oriented computing environment.

Clouds enables infrastructure as cloud compliant, the resources available in the environment are utilized non-intrusively. Cloud computing framework is harnessed to manage information system of an educational institution would be highly efficient in terms of accessibility, manageability, scalability and availability. An ad-hoc cloud enable us harness services offered by Fixed Education –cloud services created and composed within cloud system. An e-Education system doesn't fit well in the scenario.

As a solution to this problem it is seen ad-hoc cloud architecture is proposed that can rightly fit into the picture to serve the purpose. Hence the ad-hoc cloud would benefit in terms of existing service and cloud applications from the fixed cloud.

Aim of encrypted storage in cloud is to create a virtual private storage system that maintains confidentiality and data integrity while maintaining the benefits of cloud storage. In the following sections we will see the AES method used for encryption [8].

Here we have reviewed some of the issues, and set out the basis of some approaches that is step to forward in addressing security issues [9].Cloud providers often have several servers and resources in order to provide appropriate services for their users but cloud is at risk as other Internet-based technology.

II. Various Security Tricks

Before storing it at virtual location, encrypt the data with your own keys and make sure that a vendor is ready for security certifications and external audits [12] with below tricks.

1. Identity, access control, reporting of security incidents, personnel and physical layer management should be evaluated before you select a CSP (Cloud Service Provider). And you should minimize personal information sent to and stored in the cloud.

ISSN: 2005-4262 IJGDC

2. Organizations run applications and data transfer in their own private cloud and then transmute it to public cloud. While there are many issues exist in the cloud computing, Cloud Security Alliance should design relevant standards as soon as possible.
3. Open Security Architecture (OSA) provides frameworks that are easily integrated in applications, for the security architecture community. Its patterns are based on schematics that show the information traffic flow for particular implementation with policies implemented at each step for security issues.
4. Contract policies between clients and vendors are required, so that data belongs only to the client at any time, and prevent third parties to be involved at any point. Also, authentication should be backed by several methods like password plus flash card, or password plus finger print, or some combination of external hardware and password.
5. To access right Control, Security Assertion Markup Language (SAML) has been around for over 8 years now and is an excellent way of providing a Single Sign On solution across the enterprise firewall.
6. Check service level agreement. Cloud computing vendor should response about questions: what roles and responsibilities will be their? How do they verify the safety of systems? What immediate steps will be taken if there is a security breach?
7. Auditing firm should conduct interviews, observe and inspect processes and run penetration testing. The firm conducting the IT audit should have no stake one way or the other in the outcome.

III. Cryptography for Cloud

AES algorithm uses a round function that is composed of four different byte-oriented transformations:

1) Byte substitution using a substitution table known as (S-box),
2) Shifting rows of the State array by different offsets,
3) Mixing the data within each column of the State array, and
4) Adding a Round Key to the State.

In AES architecture is centrally controlled by both hardware and software. Decryption of this system is depending upon the designing rule that is called Substitution Permutation over Networking. Advanced Encryption standard has standard blocks with fixed length of 128 bits and their allowed key size is 128,192 or it can be 256 bits, new research has evolved that multiple key size can be allocated to the block it could be 32 bits with the least capacity of 128 bits and its key size may be extended no fixed length is announced that could also may vary. Operations based on the 4 by 4 matrix of the bytes with finite field calculations especially designed for the purpose of calculations. AES specifies the repetition numbers for converting the input to the normal readable text.

IV. AES Algorithm Prototype

Encryption technology is a technology for protecting data in transit to and from the cloud as well as data stored in the cloud. The aim of encryption technology is to provide safety, security to data.

In current, Microsoft allows up to seven security accounts per client and one can use these different accounts to create different zones. But available techniques are not enough to provide security to data in cloud. It is a demand and necessity of the data owners/providers/users to get high security for data. AES technique comes with 128/192/256 bits operations. In the previous section the general working of AES is explained. In this section we will see the proposed model of AES with cloud computing. Figure 1 shows the basic model . In this, data sender sends the data to AES model which applies the process to get the encrypted data which then sent to cloud service provider.

Cloud service provider will send the stored data which is in encrypted format to the requested site. At the receiver side AES model will decrypt the data.

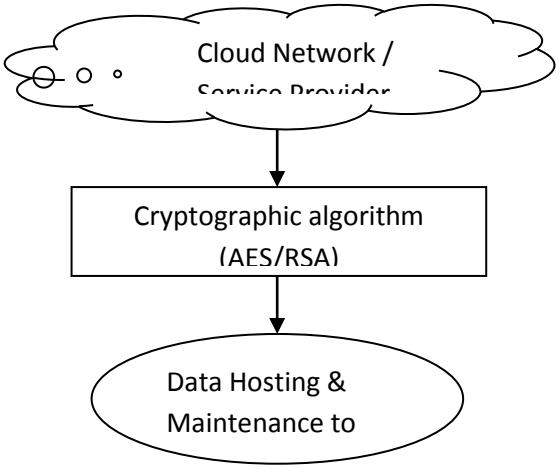

Figure 1. Cryptographic Cloud Modal

Table 1: Algorithm's Comparative Survey

ALGORITHM	GIVEN BY	KEY LENGTH	BLOCK SIZE	SECURITY RATE	EXICTION TIME
DES	IBM75	54 BIT	64 BIT	NOT ENOUGH	SLOW
AES	RIJMAN, JOAN	128,192, AND 256	128 BIT	EXELENT	MORE FAST
RSA	RIVEST, SAMIR 78	BASED ON No. of bit in N=P*Q	VARIANT	GOOD	SLOWEST
ECC	NEAL KOBLITZ	135	VARIENT	LESS	FASTEST

Table 2. Table with Comparative Security Values based on Various Authors A(Available), NA (Not Available)

Author	Cloud Security	Data Sharing	Threat	Defense Strategies	Storage Overhead	Key Size
Zhibin Zhou	A	NA	A	A	High	Linear
XiaoanXiao	A	NA	A	A	Less	Linear
ChenandZhao	A	A	A	NA	Average	
Zhou	A	NA	A	A	High	constant
Wangetal.	A	NA	NA	A	Low	Linear
Wang	A	NA	NA	A	High	Constant
Ozaetal	A	NA	NA	NA	High	Linera
SaradhyandMuralidhar	NA	NA	NA	NA	High	Constant

Butler	NA	A	A	NA	Low	Consatant
Mitchley	NA	A	A	NA	Avearage	Linear
Feldmanetal	NA	A	NA	NA	Avearage	Linear
Geoghegan	NA	A	NA	NA	Low	Constant
SahafizadehandParsa	NA	A	NA	NA	High	Linear

V. Cloud Formation Architecture

Following issues are to be handled during the formation of an ad hoc cloud.

A. Instance dynamic heterogeneity

The ad-hoc cloud might be running on different set of machines at different instances, the heterogeneity in the environment will greatly influence the design of a cloud. The Data-centre must support dynamic heterogeneity of the participating machines. Heterogeneity could be in terms of computing power shared and disk space available, RAM and n/w bandwidth on independent machines. This requires the virtualization to be highly dynamic in nature.

The ad-hoc cloud manages this issue by maintaining a table whose attributes are Node-id, MaxCPUSpeed, %CPU-usage, MAXStorage, %Storage-usage. This information is collected periodically in single phase about the P (Persistent) nodes and the V (Volunteer) nodes. Before entering the dynamic set a node allows its resources to be managed by ad-hoc Data-centre [4], and when a node exits it replicates or persists data to a persistent storage.

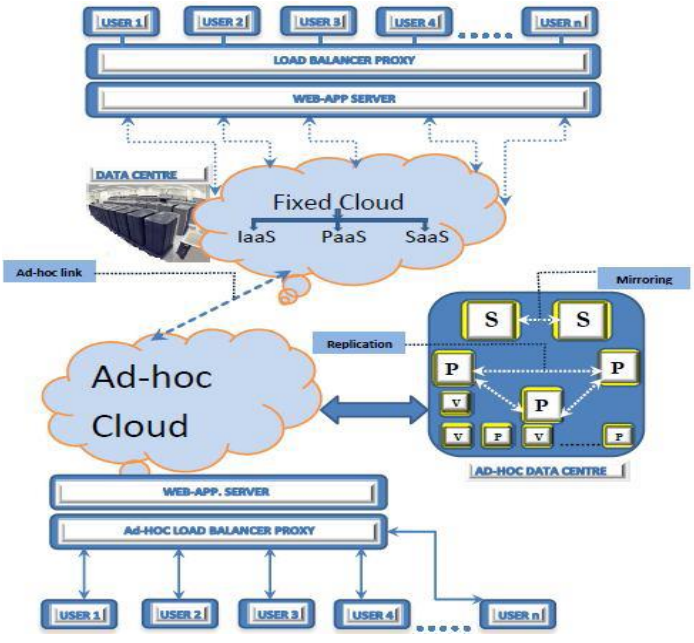

Figure 2. Ad-Hoc Cloud System

VI. Scalability and Data Management Service

Many approaches for scalability and data management services have been proposed like big table [5] and dynamo [6], but lack in providing transactional level guaranty. We use the concept of Elastras [7] which is a light weight data store capable of providing transactional level guaranty. Our data store would have Organizational level transaction manager (OLTM) and Higher level transaction manager HLTM. The transactions within an organization would be handled by OLTM and between organizations would be handled by HLTM. Elasticity at data store level is important as it would not limit upper layer for scalability. Elasticity is provided by decoupling the data base manager (DM) with the transaction manager. Application servers access the data store through load balancer for data store. For a transaction request the OLTM checks his capacity to guarantee ACID properties for a transaction, if it cannot then it forwards the request to immediate HTLM. Finally a single or collection of ODM (Organizations Database Manager) owing the database (data storage layer) commits the transaction. The Metadata Manager (MM) implementation provides decoupling of database and transaction manager and it also provides mapping of distributed database partitions into OLTM. Synchronous replication of MM is required for fault tolerance. Storage layer takes care of replication of data and fault tolerance. Slower nodes can use metadata caching for improved performance. Since HTLM are stateless therefore to improve performance during scalability spawning a new HTLM is easy. Further data base migration between data-store or in cloud can be done as discussed in Albatross [8].

VII. Need and Benefit of Ad-Hoc Cloud

Ad-hoc clouds provide necessary infrastructure and services. Due to unavailability of the fixed educational cloud at remote locations, setting up an educational organization would pose a major problem specifically in terms of the resource requirements of an educational organization. An adhoc cloud further enhances the benefits of an fixed education cloud to remote areas via an ad-hoc link. Thus provision of an ad-hoc cloud connected to the fixed cloud provides globally competitive framework, which can be harnessed by venturist with decreased cost and delay.

VIII. Conclusion & Future Work

In the entire work it is studied that the architecture of ad-hoc cloud was presented as an extended option to create cloud services for remote educational institutions. The ad-hoc cloud service running on volunteer hardware may not fit the current well-managed, pay-as-you-go cloud model, but it could open plenty of options for those who dare to enter remote locations for providing educational services. The main requirements and challenges for providing scalability and performance in a heterogeneous environment were also viewed with possible solutions to overcome some of these challenges. It is believed that ad-hoc clouds can exist as complementary infrastructures to clouds, and can even serve as a fixed cloud for many services. Behind this review work the main aim was to involve best cryptographic system to establish secure communication.

References

[1] T. Xia, Z. Li N.Yu, “Research on cloud computing based on deep analysis to typical platforms”, In: Cloud-Com '09: Proceedings of the 1st International Conference on Cloud Computing, pp. 601{608.Springer-Verlag,Berlin, Heidelberg (2009).

[2] B. Dong, Q. Zheng, M. Qiao, J. Shu, and J. Yang. 2009, “BlueSky Cloud Framework: An E-Learning Framework Embracing Cloud Computing”, In *Proceedings of the 1st International Conference on Cloud Computing* (CloudCom '09), Martin Gilje Jaatun, Gansen Zhao, and Chunming Rong (Eds.). Springer-Verlag, Berlin, Heidelberg, pp. 577-582.

[3] P. Pasatcha, K. Sunat, "A Distributed e-Education System Based on th e Service Oriented Architecture" 2008 IEEE International Conference on Web Services.
[4] OpenNebula Project: http://www.opennebula.org.
[5] F. Chang, J. Dean, S. Ghemawat, W. C. Hsieh, D. A. Wallach,M. Burrows, T. Chandra, A. Fikes, and R. E. Gruber, "Bigtable: A Distributed Storage System for Structured Data", In *OSDI*, **(2006)**, pp. 205–218.
[6] G. DeCandia, D. Hastorun, M. Jampani, G. Kakulapati, A. Lakshman, A. Pilchin, S. Sivasubramanian, P. Vosshall, and W. Vogels, "Dynamo: Amazon's highly available key-value store". In *SOSP*, **(2007)**, pp.205–220.
[7] S. Das, S. Agarwal, D. Agrawal, and A. El Abbadi, "ElasTraS: An Elastic, Scalable, and Self Managing Transactional Database for the Cloud", Technical Report 2010-04, CS, UCSB,**(2010).**
[8] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Cryptology ePrint Archive, Report2008/489, 2008, http://eprint.iacr.org/.
[9] L. Carter and M. Wegman, "Universal Hash Functions," *Journal of Computer and System Sciences*, vol. 18, no. 2, **(1979)**, pp. 143–154.
[10] J. Hendricks, G. Ganger, and M. Reiter, "Verifying Distributed Erasure coded Data," *Proc. 26th ACM Symposium on Principles of Distributed Computing*, **(2007)**, pp. 139–146.
[11] J. S. Plank and Y. Ding, "Note: Correction to the 1997 Tutorial on Reed-Solomon Coding," University of Tennessee, Tech. Rep. CS-03-504, **(2003)**
[12] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-Replica Provable Data Possession," *Proc. of ICDCS '08*, **(2008)**, pp. 411–420.

