ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Survey on Authorized Auditing of Big Data

Prof. Vijay Sonawane[1], Sachin Sidhling Kore[2], Rajendra Prakash Mane [3], Ajay Gajendra Pawar [4], Punam Dadaram Adling [5], Vaisali Chandrakant Gorhev [6]

Professor, Dept. of Computer, Bhivarabai Sawant Institute of Technology & Research Wagholi, Pune, India[1]

Student, Dept. of Computer, Bhivarabai Sawant Institute of Technology & Research Wagholi, Pune, India[2,3,4,5,6]

ABSTRACT: Cloud computing is widely spreading era. It includes IT companies, business line, all online shopping sites including cell phone service providers etc… but in other hand storage capacity and security are increasing issues. Cloud user have no more longer direct control over their data, which makes data security one of the major concerns of using cloud. Previous research work already allows data integrity to be verified without possession of the actual data file. The trusted third party known as auditor. And verification done by this auditor is known as authorized auditing. The Previous system has many drawbacks regarding third party like any one can challenge to the cloud service provider for proof of data integrity. Also in it includes research in BLSS signature algorithm to supporting fully dynamic data updates. This algorithm is used to update an only fixed-sized block known as coarse-grained updates. Though this system takes more time for updating data. We are providing a system which support authorized auditing and fine-grained update request. Thus, our system dose not only increases security and flexibility but also providing a new big data application to all cloud service providers for large data frequent small updates.

I. INTRODUCTION

Although previous data auditing schemes already have various properties potential risks and in efficiency such as security risks in unauthorized auditing requests and inefficiency in processing small updates still exist. We will focus on better support for small dynamic updates, which benefits the scalability and efficiency of a cloud storage server. To achieve this, our scheme utilizes a flexible data segmentation strategy. Meanwhile, we will address a potential security problem in supporting public verifiability to make the scheme more secure and robust, which is achieved by adding an additional authorization process among the three participating parties of client, CSS and a third-party auditor (TPA).For providing more security we are using third party authenticator. Which is able to verify our data from cloud and check our data's integrity .we are providing authenticity to the TPA using md5 hashing algorithm which is going to perform main function in our system .it will allow to achieve us the security of our data from TPA also. MD5 hashing algorithm gives 128 bit hash key which is allocate to every TPA which should be given at the time of verifying data at cloud.

II. EXISTING SYSTEM

1. Cost-efficiency brought by elasticity is one of the most important reasons why cloud is being widely adopted. For example, Vodafone Australia is currently using Amazon cloud to provide their users with mobile online-video watching services. Without cloud computing, Vodafone cannot avoid purchasing computing facilities that can process 700 rps, but it will be a total waste for most of the time.

2. Other two large companies who own news.com.au and realestate.com.au, respectively, are using amazon cloud for the same reason. We can see through these cases that scalability and elasticity, thereby the capability and efficiency in supporting data dynamics, are of extreme importance in cloud computing.

III. PROPOSED SYSTEM

The challenge/verification process of our scheme, we try to secure the scheme against a malicious CSS who tries to cheat the verifier TPA about the integrity status of the client's data, which is the same as previous work on both PDP and por. In this step, aside from the new authorization process (which will be discussed in detail later in this section),the only difference compared to is the and variable-sectored

DOI: 10.15680/IJIRCCE.2016. 0409155

blocks. Therefore, the security of this phase can be proven through a process highly similar with using the same framework, adversarial model and
interactive games defined in. A detailed security proof for this phase is therefore omitted here.

IV. SYSTEM ARCHITECTURE

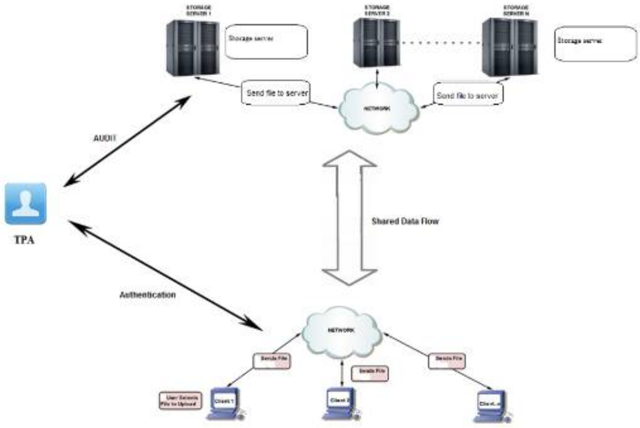

Fig. Architecture of propose system

V. ALGORITHMS

A. MESSAGE DIGESTION (MD5):

I. It Is Designed To Run Effectively On 32-Bit Processor.
II. Generate Unique Hash Value For Each Input.
III. It Produce Fixed Length 128-Bit Hash Value With No Limit Of Input Message.
IV. Advantage Is Fast Computing And Uniqueness.
V. Also Known As Hashing Function.

B. ADVANCED ENCRYPTION STANDARDS (AES)

I. Secrete Key Generation Algorithm.
II. AES Work By Repeating The Same Defined Steps Multiple Times For Encryption & Decryption.
III. It Operates On Fixed Number Of Bytes.
IV. Block Size: 128-Bit
V. Key Length: 128,192,256-Bits
VI. Encryption Primitives: Substitution, Shift, Bit Mixing.

VI. APPLICATIONS

- The client could take advantage of the entire network's processing power.
- Clients would be able to access their applications and data from anywhere at any time.

VII. CONCLUSION

Thus, in our paper we are providing a formal analysis and fine-grained data updating. Purpose of ourscheme is that fully support authorized auditing & fine-grained data updating as per request.

DOI: 10.15680/IJIRCCE.2016. 0409155

Based on our scheme we have also proposed modification that is dramatically reduce communication overheads for verification of small updates. We also plan that for further investigate on the next step how to improve server side protection methods for data security.

Hence, in our paper data security, storage and computation, efficient security plays important role undercloud computing context.

REFERENCES

1. Juels And B.S. Kaliski Jr., ‘‘Pors: Proofs Of Retrievability For Large Files,’’ In Pro. 14thacm Conf. On Comput.And Commun.Security (Ccs), 2007, Pp. 584-597.
2. H. Shacham And B. Waters, ‘‘Compact Proofs Of Retrievability,’’In Proc. 14th Int’l Conf.On Theory And Appl. Of Cryptol.AndInf.Security (Asiacrypt), 2008, Pp. 90-107.
3. R.C. Merkle, ‘‘A Digital Signature Based On A Conventional Encryption Function,’’ InProc. Int’l Cryptol.Conf. On Adv. In Cryptol. (Crypto), 1987, Pp. 369-378.
4. Hadoop Mapreduce. [Online]. Available: Http://Hadoop.Apache.Org
5. Openstack Open Source Cloud Software, Accessed On: March 25,2013. [Online].Available: Http://Openstack.Org/
6. Armbrust, A.Fox, R.Griffith, A.D.Joseph, R.Katz, A.Konwinski, G.Lee,D.Patterson,A.Rabkin,I.Stocia, And M Zaharia “A View Of Cloud Computing .”Commum,Acm,Vol.53,No.4,Pp.50-58,Apr.2010
7. Customer Presentation Of Amazom Summit Australia, Sydney,2012, Accessed On:March25,2013.[Online].Available:Http://Aws.Amazon.Com/Apac/Awssummit-Au/8. D.Boneh, H. Shachhan, And B. Lynn, ‘‘Short Signatures From The Weil Pairing,’’ J.Cryptoll., Vol. 17, No. 4, Pp. 297-319, Sept. 2004.
8. D. Zissis And D. Lekkas, ‘‘Addressing Coud Computing Issues,’’ Future Gen. ComutingSyst., Vol. 28, No. 3, Pp. 583-592, Mar. 2011.
9. G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner,Z. Peterson, and D. Song, ‘‘Remote Data Checking Using Provable Data Possession,’’ACM Trans. Inf. Syst. Security, Article 12 vol. 14,no. 1, May 2011,
10. Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, ‘‘Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage,’’IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231-2244,Dec. 2012.
11. H. Shacham and B. Waters, ‘‘Compact Proofs of Retrievability,’’in Proc. 14th Int’l Conf. on Theory and Appl. of Cryptol. and Inf.Security (ASIACRYPT), pp. 90-107 2008.