ISSN 2348 – 8034
Impact Factor- 3.155

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

Authorized Auditing Of Dynamic Big-data On cloud

(Arvind Gautam, Anjali Nalawade,Trupti Shinde, Priyanka Magar)[*1]
Prof. B.H.Thombare[2]
[*1]BE student , Department of Computer Science , Shree Ramchandra College Of Engineering , India
[2]Assistant Professor , Department of Computer Science , Shree Ramchandra College Of Engineering , India

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.

In our paper, 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.

Keywords: *Cloud computing, big data, data security, authorized auditing, fine-grained dynamic data update*

I. INTRODUCTION

Although Previous data auditing schemes already have various properties , potential risks and inefficiency 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 TPA(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. METHOD & MATERIAL

- ALGORITHM USED:

1. 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.

ISSN 2348 – 8034
Impact Factor- 3.155

iv. Advantage Is Fast Computing And Uniqueness.

v. Also Known As Hashing Function.

2. Advanced Encryption Standards (AES)

I. Secrete Key Generation Algo.

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

III. OTHER SECTIONS

(A)Motivation of the Project:

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.

(B) Purpose and Scope of Document:

For providing more security we are using TPA (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 achieving 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.

(C) Proposed System Problem Statement:

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 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.

ISSN 2348 – 8034
Impact Factor- 3.155

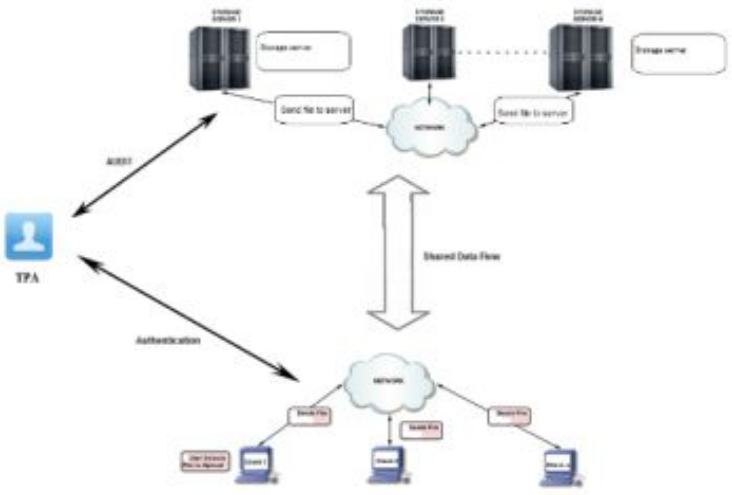

Fig. Architecture of propose system

According To Architecture We Are Having Three Main Components Viz.,

1. Client

2. Cloud Service Provider (CSP)

3. Third Party Auditor (TPA)

Functions or Authorities of Components:

1. Client

- Can create account
- Can select a file
- Can upload a file to CSS
- Can do updates in file

2. Cloud Service Provider(CSP)

- Can get file
- Can store file
- Can convert it in blocks

3. Third Party Authenticator (TPA)

- Can get a file request
- Can verity file integrity
- Can challenge to CSS

ISSN 2348 – 8034
Impact Factor- 3.155

IV. RESULT & DISCUSSION

As a result, every small update will cause re-computation and updating of the authenticator for an entire file block, which in turn causes higher storage and communication overheads.
In this project, we provide a formal analysis for possible types of fine-grained data updates and propose a scheme that can fully support authorized auditing and fine-grained update requests. Based on our scheme, we also propose an enhancement that can dramatically reduce communication overheads for verifying small updates.
theoretical analysis and experimental results demonstrate that our scheme can offer not only enhanced security and flexibility, but also significantly lower overhead for big data applications with a large number of frequent small updates.

V. CONCLUSION

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

VI. ACKNOWLEDGEMENTS

We would like to take this opportunity to thank our guide Prof.Thombare B.H. for giving us all the help and guidance we needed. We are really grateful to them for their kind support. Their valuable suggestions were very helpful. Also all staff of computer science SRCOE without whom these wouldn't accomplish.
We also grateful to Prof.Deepti Varshney, head of computer engineering department, SRCOE for his indispensable support and suggestions.

REFERENCES

[1] A. JUELS AND B.S. KALISKI JR., ''PORS: PROOFS OF RETRIEVABILITY FOR LARGE FILES,'' IN PRO. 14TH ACM 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. AND INF.SECURITY (ASIACRYPT), 2008, PP. 90-107.

[3] R.C. MERKLE, ''A DIGITAL SIGNATURE BASED ON A CONVENTIONAL ENCRYPTION FUNCTION,'' IN PROC. 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:MARCH 25,2013.[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.

[9] D. ZISSIS AND D. LEKKAS, ''ADDRESSING COUD COMPUTING ISSUES,'' FUTURE GEN. COMUTING SYST., VOL. 28, NO. 3, PP. 583-592, MAR. 2011.