© 2018 IJSRSET | Volume 4 | Issue 8 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Cloud Data Security Using Third Party Auditor

Aman Bhimrao Kamble[1], Dr. M. Y. Joshi[2]
[1]ME CNIS, MGM COE NANDED, Maharashtra, India
[2]Associate Professor Department of CSE, MGM COE NANDED, Maharashtra, India

ABSTRACT

Recently, cloud computing changed rapidly the way computing takes place. without any investment the user use cloud storage and other facilities. The user store data on remote server in the data center so there is a security problem concern to the cloud server. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. we also focused on third party auditor (TPA), on the side of the cloud client for verifying the integrity of dynamically stored data on the cloud. Through the auditing eliminates the involvement of the client. General forms of data operation supports the data dynamics such as insertion, and deletion, block modification. Cloud Computing services are not limited to archive or backup data only. so the prior work on remote data integrity frequently lacks the support of either public auditability or dynamic data operations, this paper achieves both. In this firstly we identity the direct extensions security problems with the updated data. and then show how to construct an elegant verification scheme for the seamless integration of these two salient features in our protocol design. For archiving the data dynamic efficiently, manipulating the classic Merkle Hash Tree construction for block tag authentication to improve the storage model of existing system. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multiuser setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis show that the proposed schemes are highly efficient and provably secure.

Keywords: Data storage, public auditability, data dynamics, cloud computing.

I. INTRODUCTION

Cloud computing, called on-demand computing. Data centered stored and processes users data by third-party and with their storage solutions provided to users Cloud computing allows and enterprises with various capabilities. Resources are continuously cater and freed with nominal management effort. Cloud computing is a highly demanded service or utility today due to the positive points such as high computing power, low cost of services, high performance, scalability, accessibility and availability. Distributed resources shared by using cloud computing through the network because of this the security problems are arises. The user wants secure transmission and data storage. the transmission of data are failed due to the hackers attack. The cloud computing data storage have many challenging issues that effect on the security and overall performance of the overall device[2][3].

Depository storage needs guarantees regarding the authenticity of knowledge on storage, specifically that storage servers obtain information. Its low to observe that information are altered or erased once accessing

the information, as a result of it will be late recapture lost or broken information.

Depository storage servers remain large amounts of knowledge, very little of that is fetched. They have to store information for long duration during that, there could be risk to data due to human or machine errors. Previous solutions don't fulfill these needs for proving knowledge possession. Some schemes supply a weaker guarantee through imposing storage complexity. Additionally, all present methods need the server to fetch the whole file, that isn't possible once addressing large amounts of knowledge[4].

The cloud service providers might act untrustworthily, endeavoring to cover information loss or corruption for status or economic explanations. Consequently it is good for customers to advance an effective protocol to perform periodical confirmations of their stored expertise to assurance that the cloud to be definite maintains up their knowledge adequately. As of late, regeneration codes have picked up repute considering that of their reduce restore bandwidth whilst provides fault tolerance. Regeneration Coding has been heavily used for providing high availability and reliability while launching low storage overhead in storage framework. It's a process of data security[3][5]. Regeneration Coding has been heavily used for providing high availability and reliability while launching low storage overhead in storage framework. It's a process of data security. This process secures information from damaged into fragments, improved, encoded and preclude duplicate data portions and stored across distinct areas or storage media The goal of erasure coding is to regenerate corrupted information through making use of understanding in regards to the data saved someplace else within the array in the disk storage approach.

Public auditing is the service which is used to ensure integrity of the data stored on the cloud and save the cloud users computation resources. To perform the auditing task the TPA known as third party auditor used to audit the stored data on cloud. TPA verify the correctness of the cloud data on demand without retrieving a copy of the whole data.

Our contribution:

1) Motivated the cloud computing public auditing system of data storage security and propose a protocol for supporting fully dynamic data operations.

2) We extend our scheme to support scalable and efficient public auditing in Cloud Computing. In particular, our scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA.

3) We prove the security of our proposed construction and justify the performance of our scheme through concrete implementation

II. REVIEW OF LITERATURE

In paper [1], summarizes complex systems as multi-relational networks, and enlist latent space network model to extract low-dimensional factors of sub networks and adopts likelihood ratio test to examine correlation between factors.

In paper [2], present a privacy-preserving, similarity-based text retrieval scheme that prevents the server from precisely reproducing the term composition of queries and documents, and anonymize the search results from unauthorized observers. In the meantime, their plan preserves the relevance-ranking of the search server, and empowers accounting of the number of documents that every client opens. The effectiveness of the scheme is verified empirically with two real text corpora.

In paper [3], author proposes a provable data possession model. Using this model client store the data on untrusted server for verification of the server.

In paper [4], author defined some proofs of retrievability. Because of this archive or back-up service and produce a proof the user access a target file .

In paper [5], designed a hidden space mapping a network into Euclidean space based on the connection structures of a network. Which is Compared with real geographical locations of nodes, and reconstructed locations are in conformity with those real ones. The distances between nodes in hidden space could serve as a novel similarity metric.

In paper [6], author describes the problem of the data storage and how to overcome it .In which the author used algebraic signatures hash functions for data verification and use m/n for correcting coding to protect the store data.

III. SYSTEM OVERVIEW

A. Proposed System Overview

The main three entities the cloud service provider (CSP), the TPA and the client. the architecture diagram shows the overall process. In which the firstly client send data to the cloud service provider. Then data store in to the remote server by using cloud service provider. the store file is monitored by TPA, which analysis the integrity of the stored file and report it to the client about the status of the file data. If the file data is affected, any intrusion or attacks is notified to the client using proper message flow.

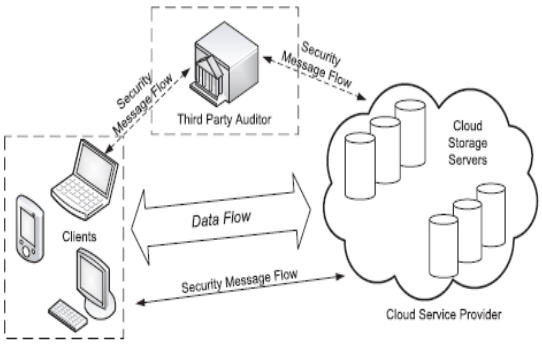


Fig. 1. Architecture Diagram

B. Mathematical Model

Protocols for Default Integrity Verification:

1. Generate the random set $\{(i, v_i)\}_{i\in I}$

$$\frac{\{(i, v_i)\}_{i\in I}}{challenge\ request\ chal}$$

2. compute $\mu = \sum_i v_i\, m_i$
3. compute $\sigma = \prod_i \sigma_i^{v_i}$
4. compute R using $\{H(m_i), \Omega_i\}_{i\epsilon I}$
5. verify $sig_{sk}(H(R))$
   and output FALSE if fail;
6. Verify $\{m_i\}_{i\in I.}$

The Protocol for Provable Data Update (Modification and Insertion)

1. Generate $\sigma_i' = (H(m_i').u^{m'_i})^{\alpha}$;
   $(M(I), i, m_i', \sigma_i')$
2. Update F and compute R'
   $(\Omega_{i,} H(m_i), sig_{sk}(H(R)), R')$
3. Compute R using $\{H(m_i), \Omega_i\}$;
4. Verify $sig_{sk}(H(R))$.
   Output FALSE if fail.
5. Compute R_{new} using $\{\Omega_i, H(m_i')\}$. verify update by checking $R_{new} = R'$. sign R' is succeed.
   $sig_{sk}(H(R'))$
6. Update R' signature.

C. Algorithm

- Key Pair Generation Algorithm:

1. Choose two random prime number, p and q.
2. Calculate r=p.q. It should be p≠q, because if p=q, then p can be obtained from the square root for r.
3. Calculate $\emptyset(r) = (p-1)(q-1)$
4. Choose public key, pk, which is relatively prime with $\emptyset(r)$.
5. Generate private key with this equation $SK.PK = 1(mod\emptyset(r))$. Note that this equation is equivalent with $SK.PK = 1 + m\emptyset(r)$, so SK can be obtained with :

$$SK = \frac{1 + m\emptyset(r)}{PK}$$

There will be an integer m, so an integer SK can be obtained. Note that SK and PK generation order are interchangeable.

- sigGen

Input: File Blocks F, secret key sk, generator g.

Output: Signature set Φ

1. Client sign each file block using secret key rsk and generator g as

$$Ti = (H(mi).g^{mi})^{sk} \; for \; i \in n$$

2. The completed set of signatures is grouped together as Φ

- proofGen

Input: Subset of file blocks mi, coefficient ai

Output: Proof P

1. The prover(server) generates the tag block T, data block M, and Auxiliary Authenticate Information (AAI) for the client to generate the MHT and confirms the root R.

2. $P = \{T, M, \{H(mi), \Omega i\}_{sl \le i \le sc}, sig_{sk}\big(H(R)\big)\}$

- verProof

Input: Proof P

Output: Boolean value {TRUE, FALSE}

1. The verifier (client or TPA) validates the proof by generating tree using AAI.

2. If step 1 is TRUE, the verifier further validate the file blocks else emit FALSE

IV. RESULT AND DISCUSSION

A. Experimental Setup Software required for the system are:

- JDK 1.8
- Netbeans Tool

B. Experimental Result

Figure 2 shows the communication overhead (server's response to the challenge) of RSA based instantiation and DPDP scheme under different block. In which we see that increase the communication cost linearly as the block size increases.

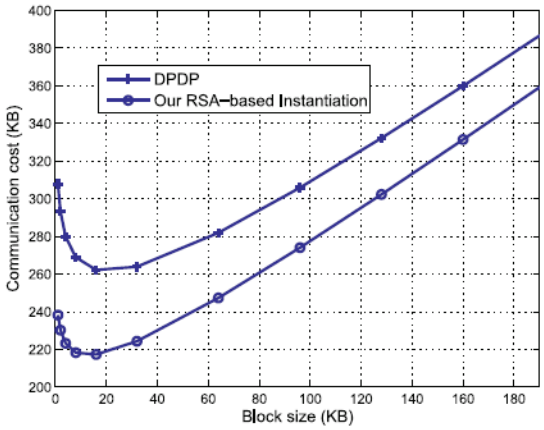
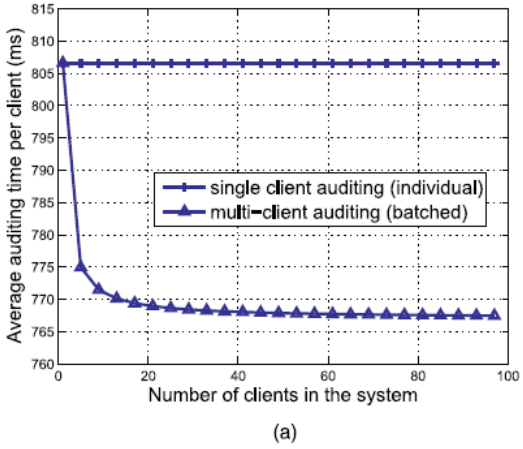
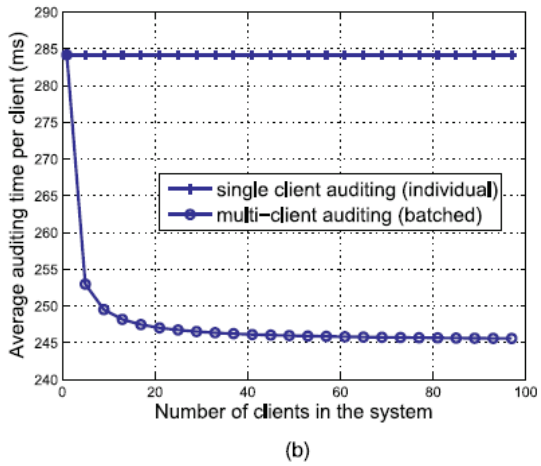


Fig. 2. Comparison of communication complexity between RSA based instantiation and DPDP , for 1 GB file with variable block sizes. The detection probability is maintained to be 99 percent.

In Fig 3 We conduct experiments for multiclient batch auditing and demonstrate its efficiency. In the system number of clients are increased. we can see, batch auditing not only enables simultaneously verification from multiple client, but also reduces the computation cost on the TPA side.



(a)



(b)

Fig 3: Performance comparison between individual auditing and batch auditing.

V. CONCLUSION

We provide the public auditability and data dynamics for remote data integrity check in Cloud Computing. we manipulating the classic Merkle Hash Tree construction for block tag authentication to improve the existing proof of storage models. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multiuser setting and multiple auditing tasks performed by TPA. From security and performance analysis prove that proposed scheme is efficient and secure.

VI. REFERENCES

[1]. C Wang, Q. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing " 2009.

[2]. Liang Duan, Charu Aggarwal, Shuai Ma, Tiejun Ma, Jinpeng Huai, "An Ensemble Approach to Link Prediction " 2017

[3]. H Pang, J. Shen, and R. Krishnan, "Privacy-preserving similarity based text retrieval "2010.

[4]. R Burns, G. Ateniese, J. Herring, L. Kissner, R. Curtmola, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores " 2007

[5]. Yi-Cheng Zhang ,Hao Liao1, Mingyang Zhou1, Zong-wen Wei1, Rui Mao1, Alexandre Vidmer1, "Hidden space reconstruction inspires link prediction in complex networks" March 2017

[6]. EL. Miller, T. Schwarz "Store Forget and Check: Using Algebraic Signatures to Check Remotely Administered Storage " 2006

[7]. C Erway, C. Papamanthou, A. Kupcu, and R. Tamassia, "Dynamic Provable Data Possession" 2009

[8]. A Juels, K.D. Bowers, and A. Oprea, "Hail: A High Availability and Integrity Layer for Cloud Storage" 2009

[9]. D Boneh, B. Lynn, and H. Shacham "Short Signatures from the Weil Pairing " 2001

[10]. R.C. Merkle "Protocols for Public Key Cryptosystems " 1980.