IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555
Vol. 5, No2, April 2015

Scalable and Secure Multicloud Data Storage Using Provable Data Scheme

B.Hema[1] , Assistant Professor / IT
R.Manikandan[2] , J.Vignesh[3], S.Venkatesan[4], , B.Tech / IT
Velammal Insitute Of Technology, Chennai

Email: [1]baluhema@gmail.com ,
[2] manikandan0106@gmail.com,[3] vigneshvicky14794@gmail.com [4] venkateshsaravanan33@gmail.com

***Abstract*— Provable data possession (PDP) is a probabilistic proof technique for cloud service providers (CSPs) to prove the clients data integrity without downloading the whole data. proposed the construction of an efficient PDP scheme for multi cloud storage. They studied the existence of multiple CSPs to cooperatively store and maintain the clients data. Then, based on homo morphic verifiable response and hash index hierarchy, they presented a cooperative PDP (CPDP) scheme from the bilinear pairings. They claimed that their scheme satisfied the security property of knowledge soundness. It is regretful that this comment shows that any malicious CSP or the malicious organizer (O) can generate the valid response which can pass the verification even if they have deleted all the stored data, CPDP scheme cannot satisfy the property of knowledge soundness. Then, we discuss the origin and severity of the security flaws. It implies that the attacker can get the pay without storing the clients data. It is important to clarify the scientific fact to design more secure and practical CPDP scheme in system architecture and security model.**

Keywords—Multi cloud,cooperativePDP , Integrity Verification, Knowledge Soundness

I. INTRODUCTION

In recent years, cloud computing has rapidly expanded as an alternative to conventional computing model since it can provide a flexible, dynamic, resilient, and cost-effective infrastructure. When multiple internal and/or external cloud services are incorporated, we can get a distributed cloud environment, i.e., multi cloud. The clients can access his/her remote resource through interfaces, for example, Web browser. Generally, cloud computing has three deployment models: public cloud, private cloud, and hybrid cloud. Multi cloud is the extension of hybrid cloud. When multi cloud is used to store the clients' data, the distributed cloud storage platforms are indispensable for the clients' data management. Of course, multi cloud storage platform is also more vulnerable to security attacks. For example, the malicious CSPs may modify or delete the clients' data since these data are outside the clients.

II. BACKGROUND AND RELATED WORK

To ensure the remote data' security, the CSPs must provide security techniques for the storage service. In 2007, Ateniese et al. [1] proposed the PDP model and concrete PDP schemes. It is a probabilistic proof technique for CSPs to prove the clients' data integrity without downloading the whole data. After that, Ateniese et al. [2] proposed the dynamic PDP security model and the concrete dynamic PDP schemes. To support data insert operation, Erway et al. [3] proposed a full dynamic PDP scheme based on authenticated flip table. Since PDP is an important lightweight remote data integrity checking model, many researchers have studied this model [4], [5], [6]. In 2012, Zhu et al. [7] proposed the PDP model in distributed cloud environment from the following aspects: high security, transparent verification, and high performance. They proposed a verification framework for multi cloud storage and constructed a CPDP scheme which is claimed to be provably secure in their security model. Their scheme took use of the techniques: hash index hierarchy (HIH), homo morphic verifiable response, and multi prover zero-knowledge proof system [8]. They claimed that their scheme satisfied the security properties: completeness, knowledge soundness, and zero-knowledge. These properties ensure that their CPDP can implement the security against data leakage attack and tag forgery attack.

In this comment, we show that Zhu et al.'s CPDP scheme does not satisfy the property of knowledge soundness. The malicious CSPs or organizer can cheat the clients. Then, we discuss the origin and severity of the security flaws. Our work can help cryptographers and engineers design and implement more secure and efficient CPDP scheme for the multi cloud storage.

Section 4 gives our attacks on Zhu et al.'s CPDP scheme. Finally, Section 5 concludes this paper. For the sake of clarity, we list some notations and their descriptions in Table 1. They will be used in this paper.

III. METHODOLOGY

To check the availability and integrity of outsourced data in cloud storages, researchers have proposed two basic approaches called Provable Data Possession and Proofs of Irretrievability. Any cloud service Provider cannot guarantee the security of inherent attacks from outside of Enterprise Cloud. The imminent threat is of Data Leakage Attack and tag Forgery Attack. As multi-tier architecture is under concern therefore computation and communication overheads are to be taken into consideration. Less the overhead cost, more preferable is the scheme. User uploading the files and then strictly to the cloud or server So, Server or Cloud are modify the content of that files easily

In this paper, we address the problem of provable data possession in distributed cloud environments from the following aspects: high security transparent Verification, and high performance. To achieve these goals, we first propose a Verification framework for multi-cloud storage along with two fundamental techniques: hash index hierarchy (HIH) and Homomorphic verifiable response (HVR). We then demonstrate that the possibility of constructing a cooperative PDP (CPDP) scheme without compromising data privacy based on modern cryptographic techniques, such as interactive proof system (IPS). Secure way to uploading and downloading the files. Server does not modified any uploading files.TPA fully verifies the file and then uploading the files to the server

IV. STRUCTURE AND TECHNIQUES

In this section, we present our verification framework for multi-cloud storage and a formal definition of CPDP. We introduce two fundamental techniques for constructing our CPDP scheme: hash index hierarchy (HIH) on which the responses of the clients' challenges computed from multiple CSPs can be combined into a single response as the final result; and homo morphic verifiable response (HVR) which supports distributed cloud storage in a multi-cloud storage and implements an efficient construction of collision resistant hash function, which can be viewed as a random oracle model in the verification protocol.

A. Multi cloud storage**:** Distributed computing is used to refer to any large collaboration in which many individual personal computer owners allow some of their computer's processing time to be put at the service of a large problem. In our system the each cloud admin consist of data blocks . the cloud user upload the data into multi-cloud.

Cloud computing environment is constructed based on open architectures and interfaces, it has the capability to incorporate multiple internal and/or external cloud services together to provide high interoperability. We call such a distributed cloud environment as a multi-Cloud . A multi-cloud allows clients to easily access his/her resources remotely through interfaces.

B. Data Integrity**:** Data Integrity is very important in database operations in particular and Data warehousing and Business intelligence in general. Because Data Integrity ensured that data is of high quality, correct, consistent and accessible.

C. Cooperative PDP**:** Cooperative PDP (CPDP) schemes adopting zero-knowledge property and three-layered index hierarchy, respectively. In particular efficient method for selecting the optimal number of sectors in each block to minimize the computation costs of clients and storage service providers. Cooperative PDP (CPDP) scheme without compromising data privacy based on modern cryptographic techniques

D. Third Party Auditor**:** Trusted Third Party (TTP) who is trusted to store verification parameters and offer public query services for these parameters. In our system the Trusted Third Party, view the user data blocks and uploaded to the distributed cloud. In distributed cloud environment each cloud has user data blocks. If any modification tried by cloud owner an alert is send to the Trusted Third Party.

E. Cloud User: The Cloud User who have a large amount of data to be stored in multiple clouds and have the permissions to access and manipulate stored data. The User's Data is converted into data blocks . the data blocks is uploaded to the cloud. The TPA view the data blocks and Uploaded in multi cloud. The user can update the uploaded data.

If the user wants to download their files, the data's in multi-cloud is integrated and downloaded.

F. Disaster Recovery**:** Back up a file system to cloud storage, using a least-common-denominator cloud interface, thus support many kinds of cloud services. It uses only one cloud to maintain one backup, and focuses on the mechanism in local file system, not the cloud platform. Wood etc . proposed a new cloud service model, i.e., disaster recovery as a cloud service, which leverages the virtual platforms in cloud computing to provide data disaster recovery service. They created a disaster recovery cloud model for web site applications which illustrated that data backup built on top of cloud resources can greatly reduce the cost of data disaster recovery.

G. Re encryption**:** In this paper, we solve this problem by proposing a time-based re-encryption scheme, which enables the cloud servers to automatically re-encrypt data based on their internal clocks. Our solution is built on top of a new encryption scheme, attribute-based encryption, to allow fine-grain access control, and does not require perfect clock synchronization for correctness**.**

V. VERIFICATION FRAMEWORK FOR MULTI-CLOUD

Although existing PDP schemes offer a publicly accessible remote interface for checking and managing the tremendous amount of data, the majority of existing PDP schemes are incapable to satisfy the inherent requirements from multiple clouds in terms of communication and computation costs. To address this problem, we consider a multi-cloud storage service as illustrated in Figure 1.

In this architecture, a data storage service involves three different entities: Clients who have a large amount of data to be stored in multiple clouds and have the permissions to access and manipulate stored data; Cloud Service Providers (CSPs) who work together to provide data storage services and have enough storages and computation resources; and Trusted Third Party (TTP) who is trusted to store verification parameters and offer public query services for these parameters.

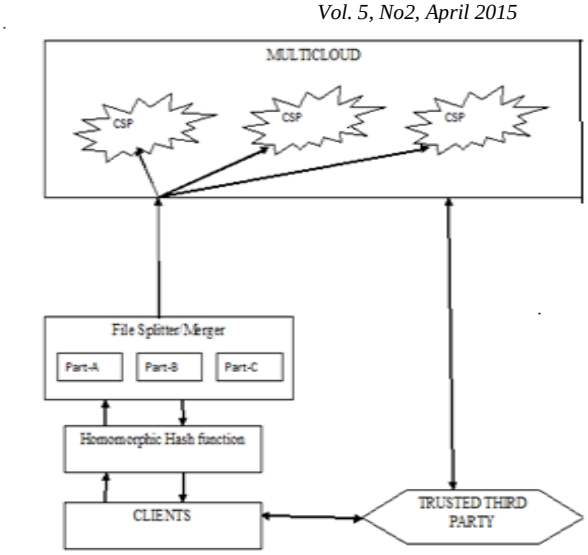

Fig.1 Methodology For Integrity

First Generate two random prime numbers, Calculate N ,derive encryption and decryptinon key from N,. User upload the file in encrypted format by using encryption key. Take a hash value and store it at third party for future verification of file integrity, Split the encrypted file by a number of CSP .Store separated files at different CSP, Give access to a right user who give a correct decryption key

A. Hash Index Hierarchy for CPDP

Hash index hierarchy representative architecture used CPDP scheme can be shown in Fig. 1. It consists of three layers: Express Layer offers the abstract representation of the stored resources; Service Layer offers and manages cloud storage services; and Storage Layer realizes data storage on many physical devices. For example, in Fig. 1, the resources in Express Layer are split and stored into three CSPs. Given a collision-resistant hash function .

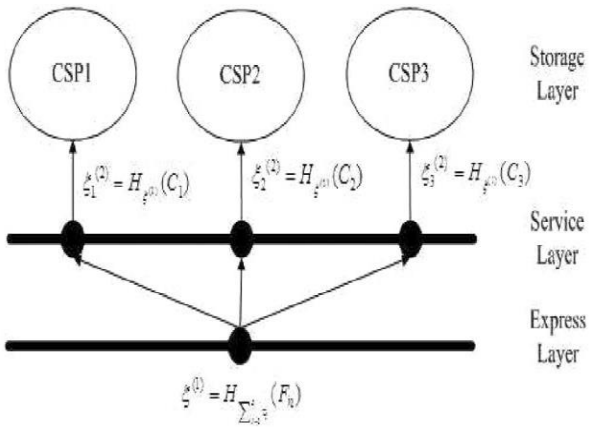

Fig.2 Collision resistant hash function

B. Homomorphic Verifiable Response for CPDP

A homomorphism is a map $f : \mathbb{P} \rightarrow \mathbb{Q}$ between two groups such that $f(g1 \oplus g2) = f(g1) \otimes f(g2)$ for all $g1, g2 \in \mathbb{P}$, where $\oplus$ denotes the operation in $\mathbb{P}$ and $\otimes$ denotes the operation in $\mathbb{Q}$. This notation has been used to define Homomorphic Verifiable Tags (HVTs) in [2]: Given two values σi and σj for two messages mi and mj , anyone can combine them into a value σ' corresponding to the sum of the messages $mi + mj$. When provable data possession is considered asMaintaining the Integrity of the Specifications Our CPDP Scheme In our scheme (see Fig 3), the manager first runs algorithm $KeyGen$ to obtain the public/private key pairs for CSPs and users. Then, the clients generate the tags of outsourced data by using $TagGen$. Anytime, the protocol $Proof$ is performed by a 5-move interactive

C. SECURITY ANALYSIS A brief security analysis of our CPDP construction. This construction is directly derived from multi-prover zero-knowledge proof system (MPZKPS), which satisfies following properties for a given assertion Completeness: whenever $x \in L$, there exists a strategy for the provers that convinces the verifier that this is the case; next Soundness: whenever $x \notin L$, whatever strategy the provers employ, they will not convince the verifier that $x \in L$; Zero-knowledge: no cheating verifier can learn anything other than the veracity of the statement. According to existing IPS research [11], these properties can protect our construction from various attacks, such as data leakage attack (privacy leakage), tag forgery attack (ownership cheating), etc

D. **Completeness property of verification**

In this scheme, the completeness property implies public verifiability property, which allows anyone, not just the client (data owner), to challenge the cloud server for data integrity and data ownership without the need for any secret information

E. **Collision resistant for index-hash hierarchy**

In our CPDP scheme, the collision resistant of indexhash hierarchy is the basis and prerequisite for the security of whole scheme, which is described as being secure in the random oracle model. Although the hash function is collision resistant, a successful hash collision can still be used to produce a forged tag when the same hash value is reused multiple times,

VI. ALGORITHM:

```
lock_resources(S)
/* S is the set of resources to lock */
  lock(LockManager)
  get timestamp
  i := 0
  while i < |S| do
    i := i + 1
    trylock(s_i)
    if could not lock s_i
      add self to s_i wait queue
      for j:= 1 to i do unlock s_j end
      unlock(LockManager) — signal HANDOFF — wait
      i := 0
    end
  end
  signal HANDOFF
  if this subsystem still holds a lock on LockManager
    unlock(LockManager)
  end
```

CONCLUSION: In this paper, we point out some flaws in Zhu et al.'s CPDP scheme for integrity verification in multicloud storage. Through cryptanalysis, we find that their CPDP scheme does not satisfy the knowledge soundness. Thus, Zhu et al.'s CPDP scheme is insecure. It is still an open problem to design secure and efficient CPDP scheme for integrity verification in multicloud storage.

References

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, 2007.

[2] G. Ateniese, R. Dipietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), 2008.

[3] C.C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 213-222, 2009.

[4] F. Sebe, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J. Quisquater, "Efficient Remote Data Possession Checking in Critical Information Infrastructures," IEEE Trans. Knowledge and Data Eng., vol. 20, no. 8, pp. 1034-1038, Aug. 2008.

[5] Y. Zhu, H. Wang, Z. Hu, G.J. Ahn, H. Hu, and S.S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," Proc. 17th ACM Conf. Computer and Comm. Security (CCS '10), pp. 756-758, 2010.

[6] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Trans. Services Computing, DOI: 10.1109/TSC.2012.35.

[7] Y. Zhu, H. Hu, G.J. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in MultiCloud Storage," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231-2244, Dec. 2012.

[8] L. Fortnow, J. Rompel, and M. Sipser, "On the Power of Multi-Prover Interactive Protocols," Theoretical Computer Science, pp. 156-161, 1988. [9] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. 21st Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '01), pp. 213-229, 2001.

[10] A. Miyaji, M. Nakabayashi, and S. Takano, "New Explicit Conditions of Elliptic Curve Traces for FR-Reduction," IEICE Trans. Fundamentals, vol. 5, pp. 1234-1243, 2001.

[11] D. Boneh, H. Shacham, and B. Lynn, "Short Signatures from the Weil Pairing," J. Cryptology, vol. 17, no. 4, pp. 297-319, 2004.