NOVEL FRAMEWORK FOR INTEGRITY VERIFICATION WITH DATA POSSESSION IN MULTI-CLOUD ARCHITECTURE

Kakulla Vinathi[1], D Usha Rani[2], Prof.S.V.Achutha Rao[3]

[1]M.Tech (CSE) Scholar, Vikas College of Engg and Tech., Nunna, Vijayawada, A.P, (India)

[2]Associate Professor, Department of Computer Science Engg.,
Vikas College of Engg and Technology, Nunna, Vijayawada, AP, (India)

[3]Professor & Head, Department of CSE,
Vikas College of Engg and Tech., Nunna, Vijayawada, A.P, (India)

ABSTRACT

The provable data procession (PDP) is a technique for the ensuring integrity of the data in the storage outsourcing. The manufacture of the effective provable data procession scheme for the distributed cloud storage to support scalability of the service and the data migration many cloud service providers to the cooperatively store and maintained the client data. In this we characterized the accommodating provable data procession scheme depend on the holomorphic verifiable reply and hash index hierarchy. WE verify the security of our scheme based on the multi power nothing knowledge proof system, in which can fulfill completeness, awareness soundness, and nothing knowledge properties. In calculation we expressive performance optimization mechanisms for our organization and in particular present an efficient method for the selecting ideal parameter values to minimize the computation costs of client's and the storage services providers (SSP). In this experiments proved that our proof introduced lower computation and communication outflows in comparison with the non-cooperative methods.

Index Terms: The Storage Security, Provable Data Possession (PDP), Interactive Protocol (IP), Zero Knowledge, Multiple Cloud and Cooperative

I. INTRODUCTION

In previously year cloud storage service has been become the faster profit growth by the providing the comparably lower cost scalable position independent platform for client data ,for the cloud computing environment is constructed based on the exposed architecture and interface, it has been the capability to incorporate multiple internal/external cloud services together to provide the high interoperability. We produced the distributed cloud environment such as the multi cloud. Frequently by using the virtual infrastructure management, the multi cloud allows the clients to easily access them resources remotely through interfaces such as a web services provided. It is happenedmore tools helpedthe cloud providers construct the distributed cloud storage platform for the managing client data. However if such important platform vulnerable to the security attacks, it would bring permanent losses to a clients. For ex. The confidential data in the enterprise might illegally accessed through the remote interface provided by the multi cloud or the relevant data and achieve may be lost or the tampered with when they are collection into the uncertain storage pool. Therefore it is necessary for cloud service providers to provide security technique for the managing their storage services. Provable data possession (PDP) in such the probabilistic solved technique for the storage provider to prove the integrity and the ownership of the client data without downloading the data. The $proof$ checking without downloading and it is especially most important for the large size file and folder. Essentially including much client files to check whether this data have tampered with or the deleted escape downloading the latest version of the data. Hence, it is not unable exchange traditional hash and signature functions in the storage our obtaining. Many provable data possession schemes have been newly proposed such as the scalable provable data possession and dynamic provable data possession. Still schemes mainly focus on provable data possession untrusted in only one storage provider and are not suitable for the multi-cloud environment.

Related Work

To check the availability and the integrity of the outsourced data in the cloud storage investigators have been proposed two fundamental characteristics known as Provable Data Possession and solved of the retrieve capacity. The proposed the provable data possession model for the insuring possession of files on the untrusted storages and provided an RSA-based scheme for the static case that achieves the communication cost. They are also proposed the widelyprovable version, which allows all, not unbiased the owner, to challenge of the server for data possession. Its property is meaning full protracted application areas ofthe provable data possession protocol due to the separation of the data owners and the users. Moreover, these schemes are insecure against replay attacks in the dynamic scenarios because of the dependencies on the index of the blocks. Apparently, they do not fit formulti cloud storage because of the loss of homomorphism property in the verification process. They support dynamic data operations, developed the dynamic provable data possession solution known as the scalable provable data possession. They proposed lightweight provable data possession scheme depends on the cryptographic hash function and symmetric key encryption, and after the server can deceive the owners by using starting metadata or the responses because of the lack of randomness in the challenges. The lot number of updates and more challenge are few of limits and fixed in the advance and users can’t perform block insertions everywhere. Based on the work, Erway et al introduced two Dynamic provable data possession schemes with the hash function tree to remember raised$(log\ n)$ communication and the computational costs for a $n - block\ file$. The basic scheme, identified as DPDP-I, recalls the disadvantage of Scalable provable data possession, and in the ‘$block\ less$ scheme identified as DPDP-II, the data blocks $\{mij\ \}j \in [1, t]$ can be leaked by response of the challengeM $= \sum$tj $= 1$ ajmij, where aj is the random challenge value. Apparently, these schemes are also inefficient for the multi cloud environment reason is the verification path of challenge block cannot be stored completely in the cloud, which relies hugely on pre-processing steps that the client conducts before sending the file to a CSP. Unfortunately, those operations prevent all efficient extension for the informing data and modifying data. Shacham and Waters (SW) proposed the improved version of this protocol known as Compact POR, in which uses homomorphic property to aggregate solve into the authenticator value and $O(t)$ computation cost for t challenge blocks, but their solution is also static and couldn’t prevent the leakage of data blocks in a verification process, presented a dynamic scheme with $(log\ n)$ cost by integrating the Compact POR schemes and the Merkle Hash Tree (MHT) into the DPDP. Furthermore, many POR schemes and models have been lately proposed including. Theannounced distributed cryptographic system that allows the set of servers to solve the provable data possession problem organization. Also in this scenario we describe a formal definition of CPDP and the essential techniques, which are developed in the construction of our scheme as well as introduce the details of cooperative provable data possession scheme for multi-cloud storage.

II. STRUCTURE AND TECHNIQUES

In this scenario, we introduced our verification framework for the multi-cloud storage and the formal definition of CPDP. In this we discussed two fundamental techniques for constructing our CPDP scheme: one is that hash index hierarchy (HIH) in this the responses of the clients' challenges computed from the multiple CSP can be combined into the single response as well as the ending results. Other is homomorphism verifiable response which support distributed cloud storage in the multicloud storage and implements the efficient construction of the collisionresistant hash function, which can viewed as the random oracle model in the verification protocol.

2.1 Verification Framework for Multi-Cloud

Probably the existing data possession scheme offer the publicly accessible remote interface for checking and managing the tremendous majority of the data and the accessible provable data possession schemes are powerless to the satisfy the inherent requirements from the multiple clouds in terms of the communication and the computation costs. In this scenario we take the multi-cloud storage service as view in the fig. In this scenario the data storage service involves three different entities: Clients who have a huge amount of the data to be stored in the multiple clouds and have the permissions to access and manipulate stored data; Cloud Service Providers who work together to provide data storage services and have sufficient storages and the computation resources; and Trusted Third Party (TTP) who is trusted to store the verification parameters and offer public query services for these parameters.

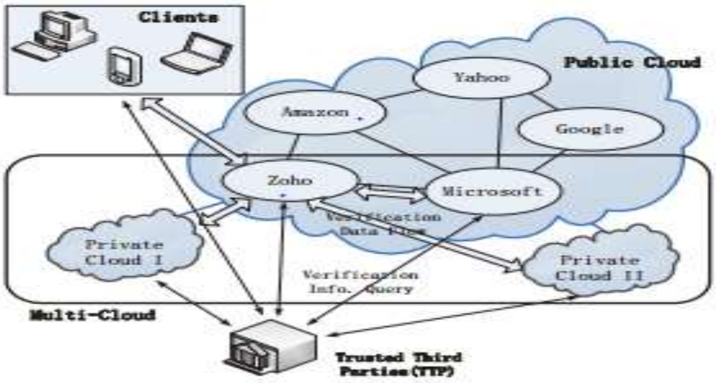

Fig. 1. Verification architecture for data integrity.

The cooperative provable data possession are integrity of the data stored on multi cloud, we proof the frameworkfor the CPDP based on the interactive proof system (IPS) and multi power zero knowledge proof system. The PDP (cooperative provable data procession)$\mathcal{S} = (KeyGen, TagGen, proof)$is the collection of two algorithms $(KeyGen, TagGen)$ and the interactive solvesystem$Proof$,$KeyGen(1_k)$take the security parameter κ as input, and retrieve the secret key sk or public secret keypair$(pk, sk)TagGen(sk, F, \mathcal{P})$, take as input secret key sk, of file F, and set of cloud storage provider$\mathcal{P} = \{Pk\}$and retrieve the triple(ζ, ψ, σ) where ζ isthe secret key inthetag$\psi = (u, \mathcal{H})$is the set of the verificationparameters$u$ and the index hierarchy of$\mathcal{H}\ for\ F, \sigma = \{\sigma(k)\}Pk \in \mathcal{P}$ denotedas set if entire tags $\sigma(k)$ is the tagof fraction F(k) of the F in the $PkProof(P, V)$ is the protocol of proof of data possessionbetween CSP($\mathcal{P} = \{Pk\}$) and the verifier (V),i.e$\langle \sum Pk \in \mathcal{P} Pk(F(k), \sigma(k)) \leftarrow\rightarrow V \rangle (pk, \psi) = \{ 1\ F = \{F(k)\}$ is intact of 0 and $F = \{F(k)\}$ is changed, where entire Pktake as a input file of $F(k)$ set where everyPk takes asa input the file $F(k)$ and the setof tags $\sigma(k)$ and the public key $pk$and the set of publicparameters ψ common input among$P$and V . Finallythe protocol run$V$ retriedthe bit $\{0 \mid 1\}$ denoting 0 and 1. Where, $\sum Pk \in \mathcal{P}$denotes cooperative computing in$Pk \in \mathcal{P}$.The trial way to realized the CPDP is to conform thedata stored in each cloud randomly ie. $\wedge\, Pk \in \mathcal{P}\ \langle(F(k),\sigma(k))\ \longleftrightarrow \rangle(pk,\psi)$,wherever$\wedge$ denotes the logical AND operations amongthe Boolean outputs of entire the protocols $\langle Pk, V\rangle$ for the entirely$Pk \in \mathcal{P}$. Still, it would cause significant communicationand computation overheads forthe verifier,aside with the loss of location transparent. Such the primitiveapproach obviously diminishes the benefitsof the cloud storage scaling arbitrarily active and deactivate ondemand. To $proof$ this problem, we extend ondefinition by adding theorganizerwhich is oneof the CSPthat directly contact with theverifier,

$\langle \sum Pk \in \mathcal{P} Pk(F(k),\sigma(k))\ \longleftrightarrow\ O\ \longleftrightarrow\ V\rangle(pk,\psi)$.

Where the action of the organizer is to pledge and organizethe verification process, Hash Index Hierarchy for the CPDP toward provisionthe distributed cloud storage and demonstrate the representative architecture used in the cooperative PDP scheme. In this hierarchy structure which resembles the natural representation of the file storage. In this hierarchical structure $\mathcal{H}$ consists of three layers to represent relationships between all blocks for stored resources.

1) The express Layers: offers the abstract representation of stored resources.

2) The service Layer: Offers and manages cloud storage services.

3) The storage Layers: introduce data storage on many physical devices.

III. COOPERATIVE PDP SCHEME

In this scenario, we propose the CPDP scheme for the multi-cloudsystem based on above mentioned structureand techniques. This architecture are constructed onthe collision resistant hash bilinear map group, aggregationalgorithm, and homomorphism responses.

3.1 Notations and Preliminaries

Let $\mathbb{H} = \{Hk\}$ be the family of the hash functions$Hk : \{0,1\} \rightarrow \{0,1\}*\ index\ by\ k \in \mathcal{K}$. In this algorithm $\mathcal{A}$ has advantageϵ in breaking collisionresistanceof $\mathbb{H}$ if $Pr[\mathcal{A}(k) = (m0, m1) : m0\ /=\ m1, Hk(m0) = Hk(m1)] \geq \epsilon$, Where the probability isover a random choices of $k \in \mathcal{K}$ and the randombits of$\mathcal{A}$. Definition. The Collision-Resistant Hash family$\mathbb{H}$ is (t,ϵ)collision-resistant if no $t$time adversaryhas advantage at least ϵ in breaking collisionresistanceof $\mathbb{H}$.

IV. SECURITY ANALYSES

We take thedeep security analysis of the CPDPconstruction. In this construction is directly derivedfrom multi prover zeroknowledge proof system which satisfies subsequent properties for the givenassertion$L$.

1) Completeness: Whenever$x \in L$, there exists thestrategy for the prover thatconvinces verifier.

2) Soundness: whenever$x\ /\!\in L$, whatever strategythe provers employ, they won't convince the verifierthat $x \in L$.

3)Zeroknowledge: No cheating verifier can be learnat entire other than the veracity of the statement.

V. PERFORMANCE EVALUATIONS

This scenario, to detect abnormality in the lowoverheadand appropriate manner, we analyze and optimizethe performance of CPDP scheme based onabove scheme from two characteristics: one is evaluation ofprobabilistic queries and other is optimization of length ofblocks. To validate the effects of the scheme, we introducedthe prototype of CPDP dependson the audit system and presentan experimental results.

5.1 Performance Analysis for CPDP Scheme

In this we present the computation cost of our CPDP scheme. We use to denote the computation costof an exponent operation inthe$\mathbb{G}$, namegx, where $x$is positive integer in $\mathbb{Z}p$ and $g \in \mathbb{G}$or$\mathbb{G}z$. We carelessnesscomputation cost of the algebraic operations are true. It is the proof method in which the proposition is proved to betrue by proving that it is impossible to be false.This article has accepted for the publication in the future issue of this abstract but hasn’t been entirely edited. Content may be change period to final publication.

5.4 CPDP for Integrity Audit Services

Depend on our CPDP scheme; we introduce the audit system architecture for outsourced data in multiple clouds by replacing the TTP with a third party auditor (TPA). In this scenario we can be constructed into the visualization infrastructure of cloud based storage service. The CPDP scheme in Hadoopdistributed file system (HDFS), which is thrdistributed, accessible and moveable file system. Hadoopdistributed file system architecture are composed of Name Node and Data Node, where Name Node maps the file name toset of indexes of blocks and Data Node indeed stores the data blocks. To protect our CPDP scheme, theindex hash hierarchy and the metadata of Name Node would be integrated together to provide the enquiry service for the hash value or index hash record χi.Depends on a hash value, the clients can developed a verification protocol way CPDP services. Therefore, it is an easy to change the check sum methods with a CPDPscheme for irregularity detection in current hadoopdistributed file system.

VI. EXISTING SYSTEM

Most existing system various source and technologies for the multi cloud, such as Platform. These tools are help the cloud providersconstruct the distributed cloud storage platform for the managing client’s data. Moreover, whether such the importantplatform is the vulnerable to security attacks, itwould like totake alongirrecoverabledamages to the client. The trusted data in theinvention may be illegally accessed through theinaccessible interface provided by multicloud data and archives maybe loss or tampered with when they are stored into the ambiguous storage pool outside the enterprise. Therefore, it is essential for cloud service providers to provide the security techniques for the managing their storage services.

VII. PROPOSED SYSTEM

To check the ability and integrity of the outsourced data in the cloud storages, researchers have proposed two basic fundamental known Provable Data Possession and other Proofs of Retrieve ability .Ateniese first proposed the PDP model for ensuring the possession of files on untrusted storages and provided the RSA based scheme for the static case that succeeds communication cost. They also commended the publicly demonstrable version, which agrees everyone, not unbiased the owner, to the challenge of the server fordata possession. They have proposed the lightweight PDP scheme depend on the cryptographic hash function and the symmetric key encryption (SKE), however the servers can be deceive the owners by using the previous metadata or responses due to the lack of randomness in contests. The numbers of the apprises and the challenges are limited and fixed in the advance and users can’t perform block insertions everywhere.

VIII. CONCLUSIONS

In this scenario we represented the construction of the efficient PDP scheme for the distributed cloud storage. Depend on homomorphism verifiable response and hash index hierarchy; we have been proposed the cooperative PDP scheme to support dynamic scalability on the multiple storage servers. In this we provide all security properties required by null information interactive solve system, hence it can be struggle various attacks even if it is deployed as the public inventory service in the cloud. Also, we optimized the probabilistic query and the periodic verification to develop an inventory performance. The obviously established that our approaches only introduce the small amount of the computation and the communication overheads. Hence, our solution can be treated as the new candidate for the data integrity verification in the outsourcing data storage systems. Separately as the futures work, we will extend this work to explore more operative CPDP constructions. Lastly, it is still the challenging problem for generation of the tags with the length of irrelevant to the size of data blocks. We could explore such an issue to provide support of the variable length block authorization.

REFERENCES

[1] B. Sotomayor, R. S. Montero, I. M. Llorente, and I. T. Foster, “Virtual infrastructure management in private and hybrid clouds,” *IEEE Internet Computing*, vol. 13, no. 5, pp. 14–22, 2009.

[2] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song, “Provable data possession at untrusted stores,” in *ACM Conference on Computer and Communications Security*, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 598–609.

[3] A. Juels and B. S. K. Jr., “Pors: proofs of retrievability for large files,” in *ACMConference on Computer and Communications*

[4] *Security*, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 584–597.

[5] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, “Scalable and efficient provable data possession,” in *Proceedings of the 4th international conference on Security and privacy in communication netowrks, SecureComm*, 2008, pp. 1–10.

[6] C. C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, “Dynamic provable data possession,” in *ACM Conference on Computer and Communications Security*, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 213–222.

[7] H. Shacham and B. Waters, “Compact proofs of retrievability,” in *ASIACRYPT*, ser. Lecture Notes in Computer Science, J. Pieprzyk, Ed., vol. 5350. Springer, 2008, pp. 90–107.

[8] Q. Wang, C.Wang, J. Li, K. Ren, and W. Lou, “Enabling public verifiability and data dynamics for storage security in cloud computing,” in *ESORICS*, ser. Lecture Notes in Computer Science, M. Backes and P. Ning, Eds., vol. 5789. Springer, 2009, pp. 355–370.

[9] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, “Dynamic audit services for integrity verification of outsourced storages in clouds,” in *SAC*, W. C. Chu, W. E. Wong, M. J Palakal, and C.-C. Hung, Eds. ACM, 2011, pp. 1550–1557.

[10] K. D. Bowers, A. Juels, and A. Oprea, “Hail: a high-availability and integrity layer for cloud storage,” in *ACM Conference on Computer and Communications Security*, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 187–198.

[11] Y. Dodis, S. P. Vadhan, and D. Wichs, “Proofs of retrievability via hardness amplification,” in *TCC*, ser. Lecture Notes in Computer Science, O. Reingold, Ed., vol. 5444. Springer, 2009, pp. 109–127.

AUTHOR PROFILE

Kakulla Vinathi, pursuing M.Tech(CSE) Vikas College of Engineering and Technology, Nunna, Vijayawada. Affiliated to JNTU, Kakinada, A.P., India

D Usha Rani, working as an Associate Professor at Vikas College of Engineering and Technology, Nunna, Vijayawada, Affiliated to JNTU, Kakinada, A.P., India

Prof S.V.Achutha Rao, is working as a HOD of CSE at Vikas College of Engineering and Technology, Nunna, Vijayawada, Affiliated to JNTU, Kakinada, A.P., India