RESEARCH ARTICLE OPEN ACCESS

Assurance of Data Integrity in Multicloud Using CPDP Scheme

Roshan R. Kolte*, Rahul Deshmukh**, Vaishali Surjuse***, Saurabh Ratnaparkhi ****
*(Department of Computer Science and Engineering, RGPV University, Bhopal)
** (Department of Computer Science and Engineering, RGPV University, Bhopal)
*** (Department of Computer Science and Engineering, RTMNU University, Nagpur)
**** (Department of Computer Science and Engineering, RTMNU University, Nagpur)

ABSTRACT
Nowadays, Cloud storage service is a faster profit growth point by providing a position-independent, low-cost platform, comparably scalable for client's data. The construction of cloud computing environment is based on interfaces and open architecture. It has cloud capable to include multiple internal and external cloud services together to provide high interoperability there can be multiple accounts associated with a single or multiple service providers. So, Security in terms of integrity is main and most important aspect in cloud computing environment.

Cooperative Provable data possession (CPDP) is a method for integrity the ensuring of data in storage outsourcing. Therefore, we address the construction of an efficient dynamic audit service and CPDP scheme for distributed cloud storage as well verifying the integrity guarantee of an entrusted and outsourced storage which support the data migration and scalability of service.

Keywords - Cloud computing, Cooperative Provable data possession, Data storage, Integrity verification, Multicloud, Proof of retrievability

I. INTRODUCTION

The main purpose of this paper is to provide security in terms of uprightness and availability of client's data which is stored on cloud. This paper will not put any load on to communication and computation and further, performance guarantee shall also be taken care of by allowing trusted third party to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional on-line burden to cloud users. Many developments are opening up the period of Cloud Computing, which is Internet-based development and use of computer and Information technology. Suppose the large size of the client's constrained resource capability and the outsourced electronic data, the center of the problem can be generalized as how can the client find an efficient. Way to perform periodical integrity verifications without the local copy of data files. Several proposal [1][2][6][7] are proposed to solve the problem. Those proposals focus on achieve the following requirements: retrievability of data, high efficiency, Stateless verification, limitless use of queries and public verification. In general, if one scheme supports private verification, it can possess higher efficiency

II. MOTIVATION

The cloud computing has been seen as the next computing has been seen as the next generation of enterprise Information and Computer Technology infrastructure, Applications, software, as a service and users will also concentrated all the information stored in the cloud data centre, this new data storage model will bring new challenges and new problems. Because the speed of today's data has produced far more than the current availability of storage devices, so there will be more and more data need to be outsource [2]. One of the main and most important and attention issues that is in the cloud computing environment, servers store data with security in terms of integrity verification. For example, storage service providers may order their own interests to hide an error to save the data more seriously, storage service providers in order to save storage space and cost, intentionally remove rarely accessed data, and then who, due to extensive confidential information, limited computing power users and outsourcing Therefore, how to backup data files in the user not the case, found an allowing users to know his information file is stored securely on the server, efficient and securely ways of good information to perform periodically verification, this data storage is cloud computing environment is an essential security issue.

III. CONTRIBUTION

Our future harmony has two main contributions:

***1) Security and Efficiency:** We* proposed by the CPDP scheme[1][2] is safer to rely on a symmetric and asymmetric key encryption will be clear, efficient in the use of SecretKeyGen and TagGen[5] algorithms. In this key exchange takes place so more secure than symmetric and asymmetric algorithm and every time parameters are generated. However, our arrangement is more efficient than the other techniques. Because it does not require the ratio [8] is more secure because we encrypt data to prevent unauthorized third parties to know its contents and no additional posts on the symbol block, and lots of data encryption in outsourced.

2) Public verifiability: To provide public validation we plan a major variation of CPDP scheme. Permit people other than the vendor for information on the server has proved challenge. However, our program than [2] is more efficient because it does not need the information for each block encryption. Framework structure paper for the rest of the paper is as follows. We describe the related work in section IV. Section V describes data integrity for cross cloud environment using CPDP to prove a structure, emphasizing the related parameters and the characteristics of CPDP. We introduce the CPDP can be publicly verifiable information to prove a structure in section VI. In Section VII security analysis of our protocol. However, Section VIII is our Result and Graph and Last Conclusion in IX.

IV. RELATED WORK

Qian Wang et al. [7] introduce a protocol for Integrity verification in Multi cloud that is provided by improving the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication. To support efficient handling of multiple auditing tasks, this paper further explore the technique of bilinear aggregate signature to extend the 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. This paper explored the problem of providing simultaneous data dynamics and public audibility and for remote data integrity check in Cloud Computing environment. This Study improves the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication. Major concern of this paper is, it is used to construct verification protocols that can accommodate dynamic data files.

Nam Yem Li et al. [2], highlights PDP scheme use for verification to avoid public verification. This paper proposed initial PDP solution to RSA based Hash function to authenticate the remote server storage data. However, due to RSA based cryptosystem the entire computing speed is slow.

Similarly Yan Zhu et al. [1], spotlight on the Cooperative Provable data possession (CPDP) scheme to verify integrity verification. This scheme is based on hash index hierarchy and homomorphic verifiable response and for data access. This paper concern, to prove the Security of scheme based on multi-prover zero knowledge proof system. CPDP scheme provides Integrity communication overheads and lower computation in comparison to non cooperative approach. However, while checking for large files, integrity is affected by the bilinear mapping operations due to its high complexity. And generation the length with tags inappropriate to the size of data blocks is a challenging task of this paper.

Then, Yan Zhu et al. [3], gives Collaborative Provable Data Possession (CPDP) scheme, where collaborative integrity verification mechanism in hybrid clouds to support the data migration and scalable service and in which we consider the reality of multiple cloud service providers to cooperatively maintain and store the client data. This paper is for a hybrid cloud is a cloud computing environment in which manages some internal Resources and an organization provides and the others provided externally. The performance optimization mechanisms scheme is acceptable and proves the security of that scheme based on multi-proven zero-knowledge proof system, which can satisfy the properties of completeness, knowledge soundness, and zero-knowledge

The protocol is similar to the CPDP, Yan Zhu [1] proposed a Proof of retrievability [1] (PORs) system, and thus the system made many verification and accurate proof, in this system, the error correction codes and sampling code and are also used To confirm the data on the verification and control, which more special place, purposes is to detect and block some random recessed special information block, and in order to protect those special blocks position, further use of asymmetric encryption technology. Compared to PORs [1], we proposed protocol requires use less bandwidth and less data storage space

In the literature [1], proposed a data storage proved cooperative Provable Data Possession (CPDP) system, which applies to of cloud in an entrusted storage server, based on Diffie-Hellman protocol systems of main plant with state verify that the label is used to check the integrity of the data stored in the cloud, which allows unlimited number of storage server authentication, and also provides a public authentication method, In which the use of public and private key system and the data must be calculated when private key matches and tags the action, making it a relatively large amount of computation. Compared to the literature [1] of CPDP protocol, the literature [3] for the previous method proposed by CPDP [1] extension of a new dynamic storage technology, because, in this new method uses the Diffie-Hellman cryptography to encrypt, making information storage, bandwidth and computational smaller, more efficient. However, we found that in the actual case, verify the number is not a difficult problem. Therefore, our protocol is based on hybrid cryptography, so our protocol than the literature [1] more efficient than the literature [3] and more security, but also increase the public verification function.

V. A INTEGRITY FOR CROSS CLOUD ENVIRONMENT USING CPDP SCHEME

In this harmony, The CPDP is based on password scheme system, the main plan is to validation of fixed-size tags, each tag are included in the block information and outsource the file before the data block encryption. Fig. 1 shows is a Cross cloud environment in CPDP agreement setting the stage diagram: Although offered CPDP schemes [1] present a publicly accessible remote interface for managing and checking the incredible amount of data, the majority of existing CPDP schemes are incapable to satisfy the inherent requirements from multiple clouds in terms of computation costs and communication. To deal with this problem, we consider a multi-cloud storage service as illustrated in Figure 1.

A. System Architecture

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

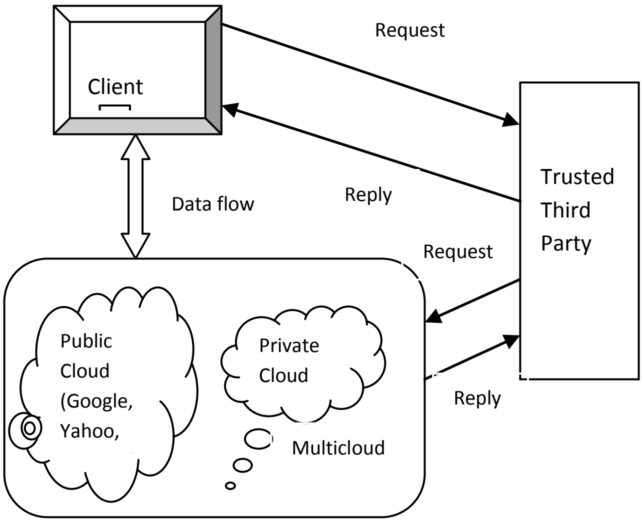

Fig1: confirmation of integrity in cross cloud Environment

In this System architecture, we think the existence of multiple CSPs to cooperatively maintain and store the clients' data. Furthermore, a cooperative PDP is used to verify the availability and integrity of their stored data in all CSPs. The confirmation procedure is described as follows: Firstly, a client (data owner) uses the secret key to pre-process a file which consists of a collection of n blocks, generates a set of public confirmation information that is stored in TTP, transmits the file and some confirmation tags to CSPs, and may delete its local copy; Then, by using a confirmation protocol, the clients can issue a challenge for one CSP to check the availability and integrity of outsourced data with respect to public information stored in TTP.

B. Protocol Directions

We neither assume that data owner has the ability to collect the evidence of the CSP's fault after errors have been found we nor assume that CSP is trust to guarantee the security of the stored data. To achieve this aim, a TTP server is constructed as a core trust base on the cloud for the sake of security. We assume the TTP is independent and reliable through the following functions: to setup and

- SecretKeyGen **(1^k):** k Takes a security parameter as input, and returns a public-secret or secret key Sk keypair (Pk, Sk);

- VeriTagGen **(**Sk,F,P**):** Takes as inputs the secret key Sk, a file F, and a set of cloud storage providers P = {Pk}, and returns the triples (S_t,V_p,A_t), where S_t is the secret in tags, V_p = (u,H) is a set of confirmation parameters u and an index hierarchy

H for F, A_t = { $A_t{}^{(k)}$ bn} Pk belongs to P) denotes a set of all tags, A_t Maintain the CPDP cryptosystem; to store and generate Data owner's public key; and to store the public parameters used to execute the confirmation protocol in the CPDP the fraction F $^{(k)}$ of F in Pk.$^{(k)}$ is the confirmation tag of scheme. Note that the TTP is not directly involved in the CPDP scheme in order to reduce the complexity of cryptosystem [1].(Cooperative-PDP).[4] A Cooperative provable data possession scheme S' is a collection of two algorithms And an interactive proof system, S' = (K, T, P):

The verification procedure is described as follows: Firstly, a client (data owner) uses the secret key (generated by proposed algorithm SecretKeyGen) to pre-process a file which consists of a collection of n blocks, generates a set of public confirmation information (generated by proposed VeriTagGen algorithm) that is stored in TTP, transmits the file and some verification tags to CSPs, and may delete its local copy. Then, by using this verification protocol, the clients can issue a challenge for one CSP to check the integrity and availability of outsourced data with respect to public information stored in TTP.

In proposed system a cooperative provable data possession in cross cloud S= (SecretKeyGen, VeriTagGen, proof) is a collection of two algorithms (SecretKeyGen, VeriTagGen) and an interactive proof system proof, as follows:

- Proof**(**P,V**):** Is a protocol of proof of data possession between CSPs (P = {Pk) and a verifier (V), that is, < Σ Pk E P P$^{(k)}$, F $^{(k)}$,V_p $^{(k)}$ (Pk, V_p,) where Pk takes input file F$^{(k)}$ and a set of tags u(k), and a public key pk and a set of public parameters V_p is the common input between P and V. At the end of the protocol run, V returns a bit {O / 1} denoting false and true.

Proposed work neither assumes that CSP is trust to guarantee the security of the stored data, nor assume that data owner has the ability to collect the evidence of the CSP's fault after errors have been found. To achieve this goal, a TTP server is constructed as a core trust base on the cloud for the sake of security. Proposed work assume the TTP is reliable and independent through the following functions [1]: to setup and maintain the CPDP cryptosystem; to store and generate data owner's public key; and to store the public parameters used to execute the verification protocol in the CPDP scheme. But the TTP is not directly involved in the CPDP scheme in order to reduce the complexity of cryptosystem. This is proposed cross cloud scheme for key generation, confirmation protocol and tag generation.

C. flow chart of future system

In this system on client side will work for two conditions for Accessing data request (ADR) and storing data request (SDR). If client want to store data, with the help of TTP Secret key is generated, by using that secret key data get stored. For accessing data, first TTP check trust between clouds and then check trusted key between client and TTP, And user will get data. As shown in fig 2, the flow chart of the future system

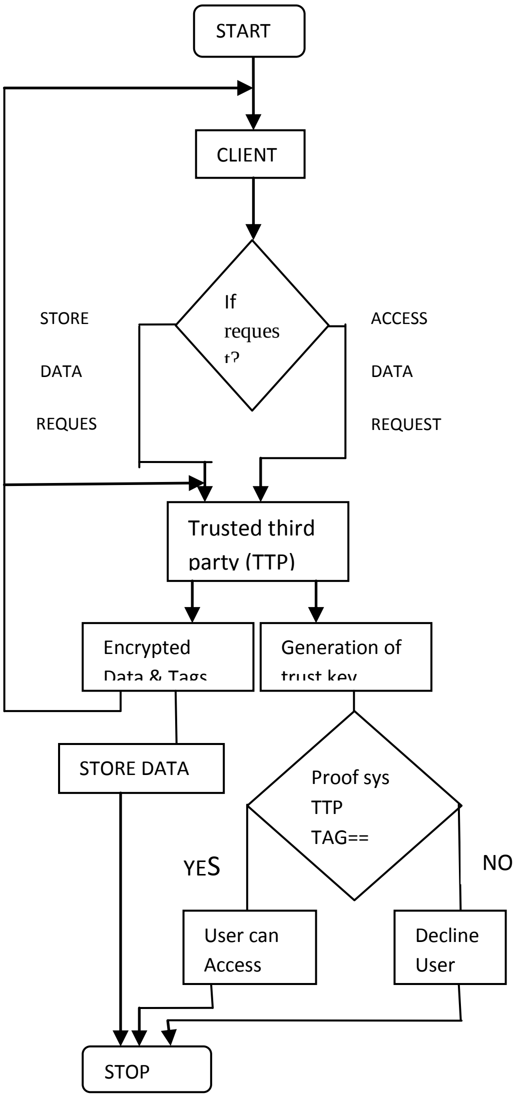

Fig:2 Flowchart for future system

VI. CPDP CAN BE PUBLICLY VERIFIABLE INFORMATION TO PROVE A STRUCTURE

If you use public confirmation, the client (owner) can be challenge (verified) phase separation, will want to confirmation task of delegate to a third party to perform, but also because the owner of a trusted third party (TTP) may have to better and more efficient than the hard computing power and physical equipment, it can improve the efficiency of confirmation. At this point, the owner do not have to produce itself verification of the server, do not have to confirmation proof of the value coming from the server, only to appoint tasks to a third party, which greatly reduce the storage costs and owner's cost of computing. Therefore, we further modify the static PDP protocol, and this stage is a hybrid variation of the static type of PDP is to provide publicly verify the characteristics of this phase can allow anyone to confirm the correctness of data stored on the server.

A trusted third party (TTP) can be calculated for each round of exchange of keys *i k* and the current challenges *i c* and to calculate the *t* times may be random challenges can be made to the server confirmation requirements. The publicly verify the hybrid static PDP hybrid verification phase of and the verification phase of the same static PDP, so we will not go into detail here.

Publicly available throughout our proposed cooperative PDP confirmation mechanism that allows information to authorized third parties for possession confirmation. However, due to the data file is encrypted by the data owner stored on the server in the cloud, so the data owners need to worry about his information in the authorized trusted third-party validation data was stolen or know the contents.

VII. SECURITY ANALYSIS

In this section will analyze the static PDP hybrid security agreement to integrity, confidentiality, and confirm the analysis of two aspects.

A. privacy

The owner of the file is stored on the server before, will use the cryptosystem to encrypt the data to ensure that the file will not be intercepted by an unauthorized person to get the file content. Because encryption and decryption *SecretKeyGen and VeriTagGen* cryptosystem uses public key and private key, security is based on calculating private key, until and unless you don’t know private key, you can’t decrypt the secret message text file M.

B. reliability

In the confirmation phase, the owner would like to confirmation secret message text *M* is a complete file stored on the server at this time, the server will calculate the value of *z* to prove he has complete store secret message text file *M*. If the server is calculated *z* calculated with the owner of the confirmation value is equal to *V*, it means the server does have the correct storage secret message text file *M*.

VIII. RESULTS AND GRAPHS

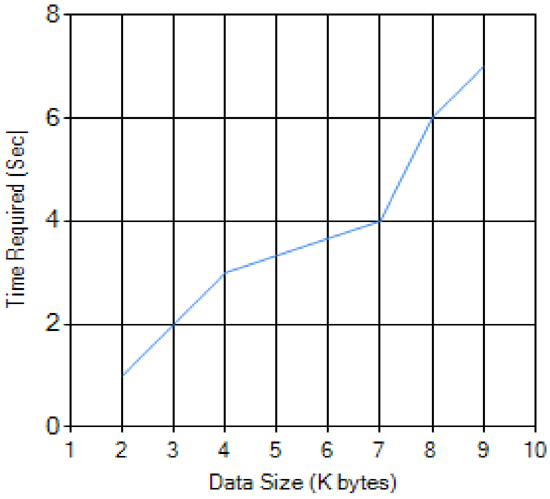

Fig 3: Graph of experimental results under different file size

Future point of view, we would enlarge our work to discover more effective CPDP constructions. First, from our experiments we found that the performance of CPDP scheme, especially for large files, is affected by the bilinear mapping operations due to its high complication. To solve this problem, RSA-based constructions may be a better choice, but this is still a challenging task because the existing RSA-based schemes have too many restrictions on the performance and security [1]. Next, from a practical point of view, we still need to address some issues about integrating our CPDP scheme smoothly with existing systems, for example, how to match index-hash hierarchy with HDFS’s two-layer name space, how to match index structure with cluster-network model, and how to dynamically update the CPDP parameters according to HDFS’ specific requirements. Finally, it is still a challenging problem for the generation of tags with the length inappropriate to the size of data blocks. We would discover such a issue to provide the support of variable-length block verification.

IX. CONCLUSION

We focused the interior issues, if an entrusted server to store customer information. We can use cooperative provable data possession scheme, which reduce the data block access, and amount of computation on the server and client. Also decreases server traffic.

Our development and design on the CPDP program is mainly based on the Public and Private Key encryption system. It exceeds what we did in the past; the improvement has brought to the bandwidth, storage system and computation. And it applied the public (trusted third party) confirmation. as a final point, we also expect our program, it supports dynamic outsourcing of information make it a more realistic application of cloud computing environment.

REFERRENCES

[1] Yan Zhu, Hongxin Hu, Gail-Joon Ahn,“ Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage” IEEE Transactions On Parallel And Distributed Systems, Digital Object Indentifier 10.1109/TPDS 2012.66 April 2012.

[2] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N.J. Peterson, and D. X. Song, “Hybrid Provable Data Possession at Untrusted Stores In Cloud Computing,” in IEEE Conference on the 7th International Conference On Parallel And Distributed Systems 10.1109/ICTPDS 2011. 70.

[3] Y. Zhu, H. Hu, G.-J. Ahn, Y. Han, and S. Chen,“ Collaborative integrity verification in hybrid clouds,” in IEEE Conference on the 7th International Conference on Collaborative Computing: Networking Applications and Work sharing, collaborate Com, Orlando, Florida, USA, October 15-18, 2011, pp. 197–206 .

[4] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, “Study on the Third-party Audit in Cloud Storage Service s,” in IEEE TRANSACTIONS ON SERVICES COMPUTING, Digital Object Indentifier 10.1109/TCS.2011.51.

[5] Qian Wang, , Cong Wang, Kui Ren, , Wenjing Lou, and Jin Li “Dynamic audit services for integrity verification of outsourced storages in clouds”, VOL. 22, NO.5, MAY 2011,1045-9219/11/$26.00 2011 IEEE. 10.1109/IMCCC.2011.135.

[6] Shu Ni-Na, Zhang Hai-Yan “On providing integrity for dynamic databased on the third party verifier in cloud computing” 2011 International Conference on Instrumentation, Measurement, Computer, Communication and Control © 2011 IEEE, DOI10.1109/IMCCC. 2011.135.

[7] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li “Enabling Public Auditability and Data Dynamic for Storage Securityin Cloud Computing” IEEE TRANSACTIONS ON Parallel And Distributed Systems, VOL. 22, NO. 5, MAY 2011