A Novel Framework for Cloud Environment Using CPDP for Data Integrity and Security

V. Narasimha Swamy[1], K. Raja Sekhar Reddy[2]

[1].*M. Tech (CSE)., Srinivasa Institute of Technology & Science, Kadapa, Andhra Pradesh*
[2]*Associate Professor, Head of the Department, CSE,Srinivasa Institute of Technology & Science,Kadapa, Andhra Pradesh.*

Abstract

In recent years, cloud storage service has become a faster profit growth point by providing a comparably scalable, position-independent,low -cost platform for client's data. Since cloud computing environment is constructed based on open architectures and interfaces. It has the capability to incorporate multiple internal and external cloud services together to provide high interoperability there can be multiple accounts associated with a single or multiple service providers (SPs).so, Security in terms of integrity is most important aspect in cloud computing environment. Cooperative Provable data possession (CPDP) is a technique for ensuring the integrity of data in storage outsourcing. Therefore, we address the construction of an efficient CPDP scheme and dynamic audit service for distributed cloud storage as well verifying the integrity guarantee of an entrusted and outsourced storage which support the scalability of service and data migration.

.

I. Introduction

Many trends are opening up the era of Cloud Computing,which is an Internet-based development and use of computer technology. Consider the large size of the outsourced electronic data and the client's constrained resource capability, the core 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. The main objective of this paper is to provide security in terms of integrity and availability of client's data which is stored on cloud. This paper shall not put any burden on to computation and communication 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.

Several schemes [1][2][7] are proposed to solve the problem. Those schemes focus on achieve the following requirements: high efficiency, stateless verification, retrievability of data, unbounded use of queries and public verification. In general, if one scheme supports private verification, it can possess higher efficiency.

II.Literature Survey

Creative writings pr is the most important step in software development process. At the advance the tackle it is principal to determine the time factor, economy n company strength. In the lead these effects satisfactory, capable next steps is to determine which operating rules and language nub be used for developing the tool. In the past the programmers mobilize structure the tool the programmers need lot of external abeyant. This support can be obtained from senior programmers, from book or from websites.

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].The cloud computing has been seen as the next generation of enterprise IT infrastructure, software, applications 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. One of the most important and most attention issues, that is in the cloud environment, servers within the data storage with security in terms of integrity verification. For example, storage service providers

may order their own interests to save the data to hide an error, more seriously, storage service providers in order to save cost and storage space, deliberately remove rarely accessed data, and then who, due to extensive confidential information, outsourcing and limited computing power users.

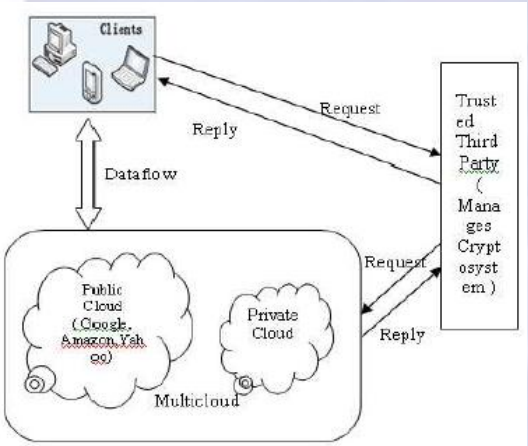

Figure 1: Verification of integrity in cross cloud environment

Therefore, how to backup data files in the user not the case, found an efficient and securely ways of good information to perform periodically verification, allowing users to know his information file is stored securely on the server, this data storage is cloud computing environment is an important security issue.

III.System Design

Our proposed agreement has two main contributions a. Efficiency and Security: the plan proposed by the CPDP [1][2] is safer to rely on a public and private key encryption will be clear, efficient in the use of SecretKeyGen and TagGen[5] algorithms. In this every time parameters are generated and key exchange takes place so more secure than symmetric and asymmetric algo. However, our plan is more efficient than the other techniques. Because it does not require lots of data encryption in outsourced and no additional posts on the symbol block, and the ratio [8] is more secure because we encrypt data to prevent unauthorized third parties to know its contents. b. Public verifiability: We plan a major variation of CPDP, to provide public validation. Allow people other than the owner 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. Paper structure Framework for the rest of the paper is as follows. In section IV, we describe the related work. Section V describes a data integrity for cross cloud environment using CPDP scheme to prove a structure, emphasizing the characteristics of CPDP and the related parameters. In section VI, we introduce the CPDP can be publicly verifiable information to prove a structure.Then, Section VII security analysis of our protocol, and VIII is about results and graphs However, Section IX is our conclusion.

IV.Related Work

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 Qian Wang et al. [7], Proposes 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 public audibility and data dynamics for remote data integrity check in Cloud Computing.

This Study mproves 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. Then, Yan Zhu et al. [3], gives Collaborative Provable Data Possession scheme, where collaborative integrity verification mechanism in hybrid clouds to support the scalable service and data migration, in which we consider the existence of multiple cloud service providers to cooperatively store and maintain the client's data. This paper is for a hybrid cloud is a cloud computing environment in which an organization provides and manages some internal resources and the others provided externally. The performance optimization mechanisms scheme is satisfactory 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.

Subsequently Yan Zhu et al. [1], focuses on the Cooperative Provable data possession scheme for integrity verification. This scheme is based on homomorphic verifiable response and hash index hierarchy for data access. This paper issued, to prove the Security of scheme based on multi-prover zero knowledge proof system. CPDP scheme provides Integrity with lower computation and communication overheads 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 of tags with the length irrelevant to the size of data blocks is a challenging task of this paper. 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. The protocol is similar to the CPDP, Yan Zhu [1] proposed a Proof of retrievability [1] (PORs) system, and thus the system made many accurate proof and verification, in this system, the sampling code and error correction codes are also used to confirm the data on the control and verification, 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 less data storage space and use less bandwidth.

V.Conclusion :

We focused the core issues, if an untrusted 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 design and development on the CPDP program is

mainly based on the usage of Public and Private keyencryption system. It exceeds what we did in the past, the improvement

References

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for vehicle-based disruption tolerant networks," in *Proc. IEEE INFOCOM*, 2006, pp. 1–11.

[2] M. Chuah and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks," in *Proc. IEEE MILCOM*, 2006, pp.1–6.

[3] M. M. B. Tariq, M. Ammar, and E. Zequra, "Mesage ferry route design for sparse ad hoc networks with mobile nodes," in *Proc. ACM MobiHoc*, 2006, pp. 37–48.

[4] S. Roy andM. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.

[5] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in *Proc. IEEE MILCOM*, 2007, pp. 1–7.

[6] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in *Proc.Conf. File Storage Technol.*, 2003, pp. 29–42.

[7] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in *Proc. WISA*, 2009, LNCS 5932, pp. 309–323.

[8] N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption," in *Proc. Ad Hoc Netw. Workshop*, 2010, pp. 1–8.

[9] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," *Ad Hoc Netw.*, vol. 7, no. 8, pp. 1526–1535, 2009.

[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption,"CryptologyePrint Archive: Rep. 2010/351, 2010.

[11] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Eurocrypt*, 2005, pp. 457–473.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Comput. Commun. Security*, 2006, pp. 89–98.

[13] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334.

[14] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 195–203.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proc. ASIACCS*, 2010, pp. 261–270.

[16] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proc. ACM Conf. Comput. Commun. Security*, 2008, pp. 417–426.

[17] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attributebased systems," in *Proc. ACMConf. Comput. Commun. Security*, 2006, pp. 99–112.

[18] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," *Comput. Surv.*, vol. 35, no. 3, pp. 309–329, 2003.

[19] S. Mittra, "Iolus: A framework for scalable secure multicasting," in *Proc. ACM SIGCOMM*, 1997, pp. 277–288.

Author's Biography

Mr. V. Narasimha Swamy was born in Proddatur, Kadapa, Andhra Pradesh in 1988., He is pursuing M.Tech, CSE in SITS, Kadapa affiliated to JNTU Anantapur, He Received B.Tech., CSE in VITS, Proddatur, Affiliated to JNTU, Anantapur. His area of interest in Cloud Computing.

Mr. K. Raja Sekhar Reddy received B.Tech degree in SSITS, Rayachoty affiliated to JNTU Anantapur. He received Master degree in CSE in the year 2011 from Arjun College of Engineering, JNTU, Hyderabad. He has 5 years experience. He is working as HOD & Associate Professor in SITS, Kadapa, Affiliated to JNTU, Anatapur.