RESEARCH PAPER | Engineering | Volume : 3 | Issue : 3 | March 2013 | ISSN - 2249-555X

Assured Protection & Veracity for Cloud Data Using Merkle Hash Tree Algorithm

KEYWORDS: Merkle Hash Tree (MHT), Cloud Storage Server (CSS), Third Party Auditor (TPA)

Mr. M. Dillibabu	Ms. S. Kumari	Ms. T. Saranya
No.81/44a,bagavathy amman street,kolathur,chennai-99	55,pettai street,anakaputhur,Chennai-600070	Plot 10 & 11, Flat F2, Bhavani Homes,Udhaya kumar nagar,mangadu, Chennai-600122

Ms. R. Preethi

1/68,Thiruvalluvar street,Kovur,Chennai-600122

ABSTRACT *Cloud Computing has been envisaged as Next Generation Architecture of IT vendor. A cloud storage system facilitates storage service with the desired collection of storage servers. Storing data in a third party's cloud system causes serious concern over data confidentiality. Encryption schemes came forward to protect the data, but limit the functionality of the storage system over the encrypted data. Constructing a secure storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority, so the Data Management and the Services are not Trust Worthy .In the proposed model, the Data Owner Sends the Data and it is Stored by splitting the Data using Merkle Hash Tree Algorithm and Verification Process is achieved for Data Safety, so that the data leakage can be prevented and requires authentication limitation to access the data in Cloud Storage Server (CSS), Third Party Auditor (TPA) is the Verifier Which Verifies the Data Block Randomly to Ensure the Trustability*

I. Introduction

SEVERAL trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the "software as a service" (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale. Meanwhile, the increasing network bandwidth and reliable yet flexible network connections make it even possible that clients can now subscribe high-quality services from data and software that reside solely on remote data centers.

Although envisioned as a promising service platform for the Internet, this new data storage paradigm in "Cloud" brings about many challenging design issues which have profound influence on the security and performance of the overall system. One of the biggest concerns with cloud data storage is that of data integrity verification at untrusted servers. What is more serious is that for saving money and storage space the service provider might neglect to keep or deliberately delete rarely accessed data files which belong to an ordinary client.

In order to solve the problem of data integrity checking, many schemes are proposed under different systems and security models in all these works, great efforts are made to design solutions that meet various requirements: high scheme efficiency, stateless verification, unbounded use of queries and retrievability of data, etc. Considering the role of the verifier in the model, all the schemes presented before fall into two categories: private auditability and public auditability. Although schemes with private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no private information. Then, clients are able to delegate the evaluation of the service performance to an independent third party auditor (TPA), without devotion of their computation resources. In the cloud, the clients themselves are unreliable or may not be able to afford the overhead of performing frequent integrity checks. Thus, for practical use, it seems more rational to equip the verification protocol with public auditability, which is expected to play a more important role in achieving economies of scale for Cloud Computing.

MHT's were initially used for the purpose of one-time signatures and authenticated public key distribution, namely providing authenticated responses as to the validity of a certificate. In a certificate revocation tree , the leaves correspond to ranges of unrevoked certificates. The tree is constructed and signed by the certification authority and then distributed to untrusted directory services. Entities wishing to verify the validity of a certificate can query such a directory service and have confidence in the correctness of a response by using the returned data to verify the certificate authority's signature. The main advantage associated with the use of MHT's in revocation schemes is that of a short proof, in turn resulting in a low communication overhead between the clients and directory services. However, the costs associated with updating the tree are rather costly. MHT's have since been applied to outsourced applications among others.

II EXISTING SYSTEM:

In the existing system, Cloud Computing has been envisioned as Next Generation Architecture of IT Enterprise but the Data Management and the Services are not Trust Worthy. So the hacker can easily hack the data of user what they are requesting from the Cloud Server. Also the hacker can modify the data.

2.1 Verification Framework for Multicloud

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 multicloud storage service as illustrated in Fig. 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.

In this architecture, we consider the existence of multiple CSPs to cooperatively store and maintain the clients' data. Moreover, a cooperative PDP is used to verify the integrity

Volume : 3 | Issue : 3 | March 2013 | ISSN - 2249-555X

and availability of their stored data in all CSPs. The verification procedure is described as follows: first, a client (data owner) uses the secret key to preprocess a file which consists of a collection of n blocks, generates a set of public verification information that is stored in TTP, transmits the file and some verification tags to CSPs, and may delete its local copy as Yan Zhu. Then, by using a 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.

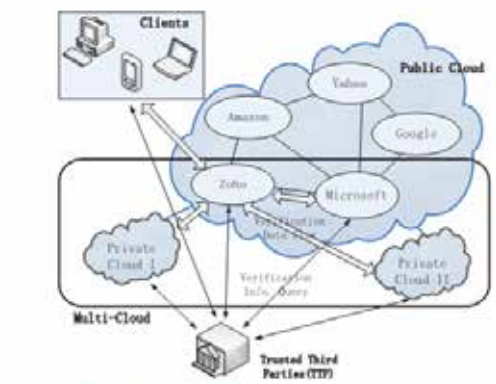


Fig. 1. Verification architecture for data integrity.

We neither assume 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. We assume the TTP is reliable and independent through the following functions to setup and maintain the CPDP cryptosystem; to generate and store data owner's public key; and to store the public parameters used to execute the verification protocol in the CPDP scheme. Note that the TTP is not directly involved in the CPDP scheme in order to reduce the complexity of cryptosystem.

III PROPOSED SYSTEM:

In the proposed system, the Data Owner Sends the Data and it is Stored in Cloud Storage Server (CSS). Third Party Auditor (TPA) is the Verifier Which Verifies the Data Block Randomly to Ensure the Trustability. The Data is Split Using Merkle Hash Tree Algorithm and Verification Process is achieved for Data Safety. The modification that We Propose is the Verification is Achieved Using Password, IP Address and Mac Address of the user who is requesting the data. So that

we can ensure and the data will be accessed by the prominent user. The hacker will be identified easily.

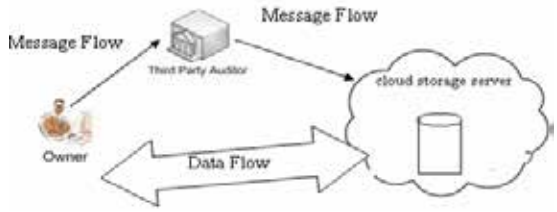


Fig 2:Third Party auditor

Multiple clients can store the data in the cloud server in the presence of Third Party Auditor for the future use, named as Cloud Storage Server(CSS). The interaction begins from the client to the Cloud Storage Server in an orderly manner.

i) Client send the data to the CSS.
ii) The data is accepted by CSS and stored by splitting it by using Merkle Hash tree algorithm to provide confidentiality and assure data integrity.
iii) The Third Party Auditor will verify the user with the help of the following parameters namely password, IP Address and MAC Address.
iv) If TPA verifies the user as an authenticated user then it grants the permission to avail the data services.
v) Data loss can be prevented by doing the verification at the end of the process.

3.1 Data Splitting using Merkle Hash Tree

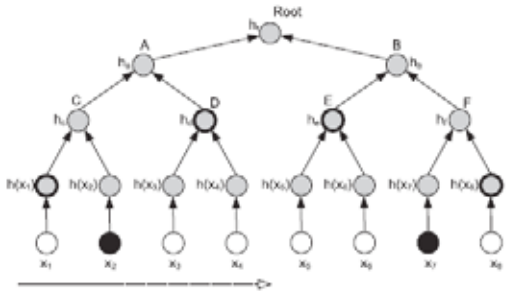
The binary search tree has been constructed using an set of ordered values.To build the tree, leaves hold the ordered elements in the set, and have each leaf node contain the hash value of its element as Einar et.al(2006). Therefore, a leaf associated with element xi will contain the value h(xi),where h() is a cryptographic one-way hash function, uses SHA-1 and To proceed up to the next level, the internal nodes will be created with the corresponding hash values. With the hash values, the node can do the concatenation for the upcoming children. Order can be identified for the internal nodes using the hash values. An internal node whose children are, let v1 and v2 be the children of the internal nodes holding the hash values. Repeat these process until a tree has been built with the higher level, so that the root node is digitally assigned with the values.

Fig 3: Data Splitting Using Merkle Hash Tree

3.2 User Authentication using Third Party Auditor

The third party auditor is the person (other than the Data owner) who will verify those data that are stored in the cloud server. The third party auditor will be the authorized person who is appointed by the Data Owner.

The TPA will maintain all the information about the client specifically IP address, MAC Address and the root tool kit(where the registered user name and the password will be stored). TPA will generate unique ID using the above mentioned parameters for the registered users. Thus it identifies the authenticated user and prove the trustability.



3.3 Data Verification and Integrity

Data integrity is verified by the CSS after the TPA assure that the user is an authenticated user and then reveals the splitted data in to an service and make them to arrange in an orderly manner to obtain the original data.

IV Conclusion and future work

In this paper we contributed our work towards the ensured data integrity and verification in the cloud system. To avoid the data duplication and data lost we utilized Merkle hash tree for data splitting in an advanced manner. Here the third party auditor is utilized as an interface between the CSS and Client so that the Data can't be viewed by the TPA. Only the verification has been done by using the parameters such as the password, IP address and MAC Address to identify the trusted user.

As part of our future work we extend additional security for the data by sending it in an video file which olds the encrypted and spitted data in the moving stream.

Volume : 3 | Issue : 3 | March 2013 | ISSN - 2249-555X

REFERENCE [1] Einar Mykletun , Maithili Narasimha & Gene Tsudik "Providing Authentication and Integrity in Outsourced Databases using Merkle Hash Tree's", ACM Transactions on Storage (TOS) Volume 2 Issue 2, May 2006. | [2] Goodrich.M.T. & Tamassia.R, "Efficient authenticated dictionaries with skip lists and commutative hashing in Technical Report" ,Johns Hopkins Information Security Institute, 2000. | [3] Hacig¨um¨us.H„, Iyer.B, Li.C, & Mehrotra.S, Executing sql over encrypted data in the database-service-provider model,. in ACM SIGMOD Conference on Management of Data, pp. 216.227, ACM Press, June 2002. | [4] Hacig¨um¨us.H„, Iyer.B, and Mehrotra.S, "Providing database as a service", in International Conference on Data Engineering, March 2002. | [5]Martel.C,Nuckolls.G, Devanbu.P, Gertz.M, Kwong.A, & Stubblebine.S.G.,A general model for authenticated data structures, 2001. | [6] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Mengyang Yu "Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage," IEEE transactions on parallel and distributed systems, vol. 23, no. 12, december 2012.