SECURE FILE SHARING OF DYNAMIC AUDIT SERVICES IN CLOUD STORAGE

N.Vidhya[1], P.Jegathesh[2]

[1]Student M.E (CSE), Oxford Engineering College, Trichy, India
[2]Assistant professor (CSE), Oxford Engineering College, Trichy, India

Abstract

Data integrity and storage efficiency are the two important requirements for cloud storage. Authorized users access the data and share the files in secure manner. The cloud storage service (CSS) relieves the burden for storage management and maintenance. Fragment Structure, random sampling and index table is used to construct the Audit service. These techniques are supported provable updates to cloud outsourced data. The third party auditing allow to save time and computation resources with reduced online burden of the user. Probabilistic query and periodic verification for improving the performance of audit services and also audit system verifies the integrity.

Keywords: *Cloud Storage Service, Proof of Data Possession, Cloud Service Provider, Third Party Audit, Public Verification Parameter.*

--*--**

1. INTRODUCTION

Cloud computing provides computing resources, utilities are provided to the users via internet. Cloud is a model for accessing user data's, on demand network services to access the secure data. It maintains the shared pool of configurable computing resources. Now a day's many software industries used the cloud computing services to secure their data's. It is used to pay per uses and it does not need any software to install the user. Cloud computing services are classified into three parts: IaaS(infrastructure as a service), SaaS(software as a service) and PaaS(platform as a service). First service provides access to computation resources as per user basis. Second service is a simple application; it is delivered to thousands of users from the resource pool. Third service uses the building blocks of the vendor's deployment environment. If the user need to access the data from shared pool, the administrator verifies the user is authorized person to take the data.

Cloud data storage services involves four entities.(i)Administrator controls the user details, file insertion, file access, file deletion and the time of user presents in the network to access the cloud data's. (ii)Third party auditor checks the correctness of cloud data. Some techniques are used to establish the auditing concepts. (iii) Users access the cloud data as per demand services. Users retrieve more useful information from multiple repositories and no limitation to access the particular storage part in the shared pool.

2. BACKGROUND & RELATED WORKS

Cloud-based outsourced storage [1] reduced the client's burden for storage management and maintenance by providing a comparably low-cost, scalable, location-independent platform. To avoid the security risks, audit services are critical to ensure the integrity and availability of outsourced data and to achieve digital forensics and credibility on cloud computing. Provable data possession (PDP) is a cryptographic technique to verify the integrity of data without retrieving it from unauthorized servers. Probabilistic queries and periodic verification, as well as an optimization method of parameters of cloud audit services are implemented to provide secure access. This technique reduced the workload on the cloud storage servers.

The third party auditor (TPA) [2] verifies the integrity of the dynamic data stored in the cloud. The TPA reduces the involvement of the client through the auditing of whether his data stored in the cloud storage. It is an efficient method to secure the user's data using Third party auditor but it may leak the data to send the linear combinations of data blocks to the auditor. The data may be stored temporarily while being authorization process. Store and forward transactions processed after complete the authorization.

POR[5] protocol is designed to protect a static archived file in cloud storage. Critical information stored as storage-as-a-service in encrypted format. It is more flexible and cost effective storage environments. PORs lead to a number of possible researches in the future. The classic merkle hash tree constructed for block tag authentication to achieve secure cloud storage and data dynamics.

3. PROPOSED SYSTEM

User easily access the secure cloud storage system is constructed with administrator, Third party auditor and cloud servers. Auditing technique verifies the integrity verification of cloud data storage. Administrator controls the user access of unauthorized party.

System Architecture

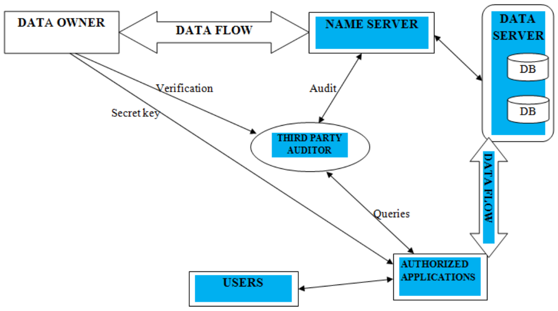

Fig 3.1 System architecture of the proposed system

3.1 Module 1: Key Generation

The owner generates the public/secret key pair (pk, sk) by system manager. The secret key is not visible and then sends the public key (pk) to TPA. Data owner provides the access to authorized users and shares the public key.

3.2 Module 2: Tag Generation

The user's/clients use the secret key (sk) to pre-process a file in cloud storage. It consists of a collection of n blocks, generates a set of public verification parameters and index-hash table. User data's are stored in TPA (Third party auditor) and transmits the file with some verification tags to CSP (Cloud service provider).

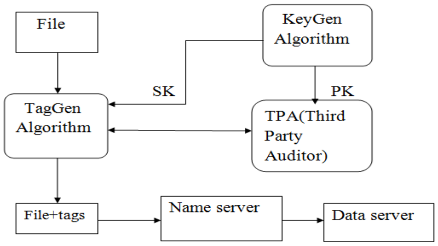

Fig 3.2 Tag generation

3.3 Module 3: Periodic Sampling Audit:

TPA (Third party auditor) challenges to audit the integrity and availability of outsourced data stored in TPA. Audit process detects some errors in secure storage of unauthorized modification. It consists of two concepts: Verification and Authorization. Administrator collects all the user details within the cloud server. Verification process is constructed with interactive proof protocol of cloud storage.

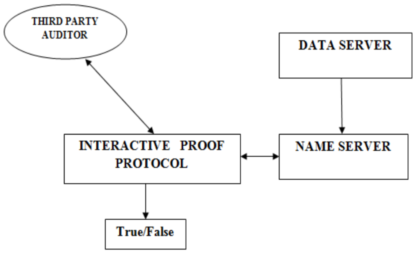

Fig 3.3 Periodic Sampling Audit Flow

3.4 Module 4: Audit for Dynamic Operations:

Authorized application holds the secret key (sk) and it can manipulate the index hash table stored in TPA. TPA cannot cheat the authorized application and audit records. User inserts the files in cloud storage with authorized permission from administrator.

Dynamic Data Operations:

Insert operation: User inserts the file in cloud storage. The file is stored in Encrypted data format. Audit process audits the file in secure techniques.

Update operation: It is an algorithm of Authorized applications update the block of a file. It updates the data's only trusted parties.

Delete operation: After verify the user is authorized the TPA gives the permission to delete the file in cloud storage.

Insert (sk, Xi, mi) is an algorithm run by AA to insert the block of a file mi at the index i by using sk, and it returns a new verification metadata.

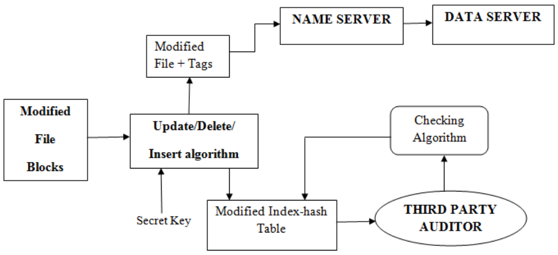

Fig 3.4 Flow of dynamic data operation

Checking algorithm tests the audit process is controlled by Administrator. The User data application invokes the Update, Delete, and Insert algorithms, and then sends to TPA and CSP, respectively. It is important to ensure the audit process of

TPA. Finally, Admin gives the permission to modify audit records after the confirmation message from CSP is received.

4. CONCLUSIONS

Cloud Storage requirements of data integrity and storage efficiency proposed based on these auditing techniques. Audit service constructed based on secure technique of PDP and verification process achieved. Comparing other techniques to construct the audit search is less than this technique. It increased the data integrity of the cloud storage and avoids the hackers to access the storage process. File insertion, File updating, File deletion is possibly used to authorized users. Cloud service provider offered an audit service to audit the integrity and availability of Secure Storage Pool.

REFERENCES

[1]. Yan Zhua,b, Hongxin Huc, Gail-Joon Ahnc, Stephen S. Yauc **,"Efficient Audit Service Outsourcing For Data Integrity In Clouds"**,In The Journal of Systems and Software 85 (2012) .

[2]. Wang.Q, C. Wang, K. Ren, W. Lou, and J. Li, **"Enabling Public Audit Ability And Data Dynamics For Storage Security In Cloud Computing",** In IEEE Trans. Parallel Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[3]. Cong Wang, Student Member, IEEE, Sherman S.M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE, **"Privacy-Preserving Public Auditing For Secure Cloud Storage".**

[4]. Abhishek Mohta* ,Ravi Kant Sahu,Lalit Kumar Awasthi ,Dept. of CSE, NIT Hamirpur (H.P.) India**,"Robust Data Security For Cloud While Using Third Partyauditor"**

[5]. Juels.A and J. Burton, S. Kaliski, **"Pors: Proofs Of Retrievability For Large Files"**,In Proc. ACM Conf. Computer and Comm. Security (CCS'07), pp. 584-597, Oct. 2007.

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

[7]. Govinda.K, V.Gurunathaprasad, H.Sathishkumar,**"Third Party Auditing For Secure Data Storage In Cloud Through Digital Signature Using RSA"**, In International Journal Of Advanced Scientific And Technical Research(Issue 2, Volume 4- August 2012) Issn 2249-9954.

[8]. Ezhil Arasu.S, B.Gowri, S.Ananthi **,"Privacy-Preserving Public Auditing In Cloud Using HMAC Algorithm ",**In International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-2, Issue-1, March 2013 .

[9]. Shingare Vidya Marshal **,"Secure Audit Service by Using TPA for Data Integrity in Cloud System"**,In International Journal of Innovative Technology and Exploring Engineering (IJITEE)ISSN: 2278-3075, Volume-3, Issue-4, September 2013.

[10]. Jiawei Yuan,Shucheng Yu **"Secure and Constant Cost Public Cloud Storage Auditing with Deduplication",** University of Arkansas at Little Rock, USA.

[11]. Jiawei Yuan, Shucheng Yu**,"Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud",**University of Arkansas at Little Rock ,USA.

[12]. Jeyadevan.S, Dr.S.Basavaraj Patil, S.Saravanan, Naina Kumari, **"Introducing Various Algorithms To Make The Data-Storage In Clouds Secure",**In International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012.

[13]. Vijeyta Devi & Vadlamani Nagalakshmi,**"A Prospective Approach On Security With RSA Algorithm And Cloud SQL In Cloud Computing",** In International Journal Of Computer Science And Engineering (Ijcse) Issn 2278-9960 Vol. 2, Issue 2, May.

[14]. Vidhisha.S, C.Surekha, S.Sanjeeva Rayudu, U.Seshadri**," Preserving privacy for secure and outsourcing for Linear Programming in cloud computing",** Jawaharlal Nehru Technological University Ananatapur.

[15]. V.Venkatesh, P.Parthasarathi**," Enhanced audit services for the correctness of outsourced data in cloud storage "**,In International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2.

[16]. Wang, Qian Wang, Kui Ren, Ning Cao, And Wenjing Lou, **"Toward Secure And Dependable Storage Services In Cloud Computing",**In IEEE Transactions On Services Computing, Vol. 5, No. 2, April-June 2012.

[17]. Q. Wang, K. Ren, W. Lou, and Y. Zhang, **"Dependable and secure sensor data storage with dynamic integrity assurance,"** in *Proc. Of IEEE INFOCOM'09*, Rio de Janeiro, Brazil, April 2009, pp. 954–962

[18]. K. D. Bowers, A. Juels, and A. Oprea, **"Hail: A high-availability and integrity layer for cloud storage,"** in *Proc. of CCS'09*. Chicago, IL, USA: ACM, 2009, pp. 187–198.