ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Secure Auditing For Outsourced Data in Cloud Using Homomorphic Token and Erasure Code

N.S. Monalisa Devi[1], T. Sounder Rajan[2]

M.E. Department of CSE, K S R College for Engineering and Technology, Tiruchengode, TamilNadu, India[1]

Associate Professor, Department of CSE, K S R College for Engineering and Technology, Tiruchengode, TamilNadu, India[2]

ABSTRACT: Cloud Computing is the process of providing computer resources like hardware and software as a service on-demand. It also provides remote services with a user's data and software Cloud Computing is the result of evolution and adoption of existing technologies and paradigms. The existing work presented a dynamic audit service for verifying integrity of un-trusted and outsourced storage. Audit service is constructed based on fragment structure, random sampling and index-hash table. Support provable updates to outsourced data and timely anomaly detection. Probabilistic query and periodic verification method is introduced. In proposed, secured auditing system for cloud data storage with Error Corrections Guarantees Storage using homomorphic token and distributed erasure-coded data. Allows users to have audit cloud storage resistance to threats for auditing with minimal communication and computation cost.

KEYWORDS: periodic sampling, Index hash table, Homomorphic token, Erasure code.

I. INTRODUCTION

Cloud computing is the delivery of computing as a service rather than a product whereby shared resources, software and information are provided to user as a utility (like the electricity grid) over a network. In cloud computing, storage plays the major role. Cloud storage is the service model in which data is maintained, managed and backup remotely made available to user over a network. The main features of cloud storage are remote access and file archiving, automatic updates, incremental backups, file sharing, etc. Some of the cloud service providers are Amazon, Google, Microsoft azure service, etc. Integrity verification of outsourced data is done by dynamic audit services. Interactive Proof System (IPS) provides auditability without any raw data and protects the data privacy. User authentication is maintained by providing secret key to the user and public key to the Third Party Audit (TPA). Auditing result ensures strong cloud storage correctness guarantee to achieve fast data error localization that identifies of misbehaving server. Homomorphic token have computation function belongs to a family of universal hash function and preserve the homomorphic properties.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

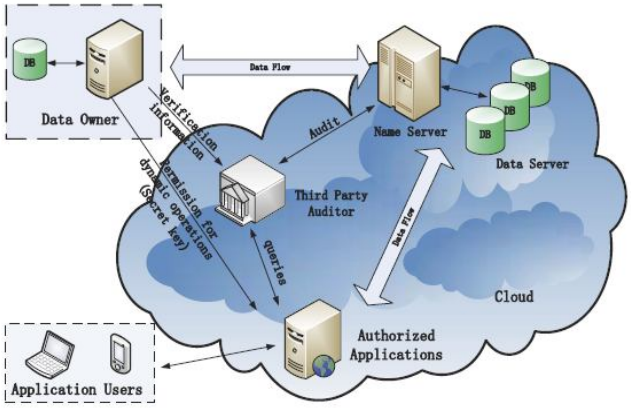
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014



Cloud Outsource Data Storage

II. EXISTING SYSTEM

Cloud outsource data storage service involves four entities Data Owner (DO) and large amount of data to be stored in the cloud. Cloud Service Provider (CSP) provides data storage service and has enough storage space and computation resources. Third Party Auditor (TPA) manage or monitor the outsourced data under the delegation of DO Authorized Applications (AAs) right to access and manipulate the stored data.

Application users utilize various cloud application services via AAs. TPA is reliable and independent throughout the audit functions. TPA makes regular checks on integrity and availability of delegated data at appropriate intervals. TPA able to organize, manages, and maintains outsourced data support dynamic data operations for AAs. TPA takes evidences for disputes about inconsistency of data in terms of authentic records for all data operations. The techniques used are

i) Fragment Structure and Secure Tags
ii) Periodic Sampling Audit
iii) Index Hash Table

i) Fragment Structure and Secure Tags

Files are combined with tags to improve the performance. The file 'F' is split into 'n' blocks i.e., $\{m_1, m_2, \ldots, m_n\}$. Each block again split into 's' sectors i.e., $\{m_{i1}, m_{i2}, \ldots, m_{is}\}$. The fragment consists of 'n' block-tag pair (m_i, σ_i) and it is stored in cloud service provider, where m_i is the file blocks and σ_i is the signature tag.

ii) Periodic Sampling Audit

Checking of the data is done periodically.Periodic sampling greatly reduces the workload of audit services. A randomly chosen challenge $Q=\{(i,v_i)\}_{i\in I}$ where I is subset of the block indices, v_i is a random coefficient.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

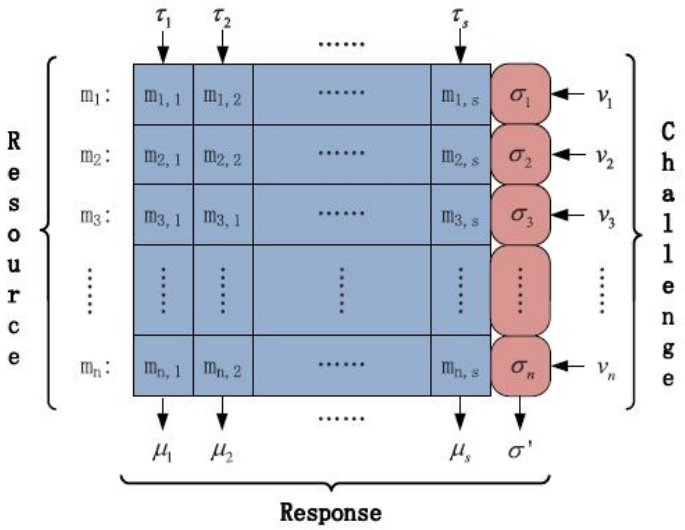
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014



Fragment Structure And Sampling Audit

iii) Index Hash Table

File changes are recorded and generate hash value for each block. IHT consists of serial number, block number, version number and random integer. All records in IHT differ from one another to prevent the forgery of data blocks and tags.

IHT with Random Values

No.	B_i	V_i	R_i	
0	0	0	0	← Used to head
1	1	2	r_1'	← Update
2	2	1	r_2	
3	4	1	r_3	← Delete
4	5	1	r_5	
5	5	2	r_5'	← Insert
⋮	⋮	⋮	⋮	
n	n	1	r_n	
n+1	n+1	1	r_{n+1}	← Append

Index Hash Table

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

DISADVANTAGES OF EXISTING SYSTEM

Secured auditing was not addressed against threats because of both internal and external attack. Sampling audit is efficient for outsourced data but it was not suitable for irregular data. Ambiguity arises in correctness of the data storage in cloud due to absence of auditing. The lack of rigorous performance analysis for a constructed audit system greatly affects the practical application of their scheme. Unable to handle data error localization for the files stored in cloud. Server may remove the client content from cloud, those misbehaving server activities were hidden.

III. PROPOSED SYSTEM

In cloud, the data are not present at user place because it is stored at cloud server. It may lead to some security threats mainly internal attack and external attack. Internal attack comes from the cloud server itself, server may be malicious and hide some data loss issues due to byzantine failure. External attackis from outsiders, may lead to modification of data or deleting the user.

To avoid these threats a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data assures a trusted and secured cloud storage service. It audits the storage integrity, using and homomorphic tokens and erasure coded data. This not only audits the correctness of data in cloud, but also on the error localization, i.e., the identification of misbehaving server. The identification of corrupted server is done instantly, which helps in easy retrieval of data. The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost.

Homomorphic token is the conversion of data into cipher text that can be analyzed and worked with as it were still in its original form. For example, we take the number as 15. In cloud storage it is stored as follows. First it is split into 5+10=15. Each element in the set is multiply by 2 and it forms the new set as 10 and 20 and it is stored as 30 (i.e.,) 10+20=30. Decryption is done by dividing the new set by 2 (i.e.,) 30/2=15.

Erasure encoding is a method of data protection in which data is broken into fragments, expanded and encoded with redundant data pieces and stored across a set of different location such as storage nodes, disk.

"n = k + m"

where'k' is the original amount of data,
'm' is the extra data or symbol added to provide protection,
'n' is the total number of data created after the erasure coding process.

ADVANTAGES OF PROPOSED SYSTEM

Strong cloud storage correctness is assured by means of frequent auditing for outsourced data. The audit performance is maximized and it makes more efficiency for the outsourced data. It provides higher assurance to monitor the behavior of an untrusted cloud service provider. Tag generation helps to find the cloud data error localization quickly. With the help of error localization, each response is computed exactly in the same way as token and the user simply find which server is misbehaving.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

IV. SYSTEM MODULES

- Cloud Outsource Storage Services
- Tag Generation
- Periodic Sampling Audit and Dynamic Operation
- Correctness Verification and Error Localization
- File Retrieval and Error Recovery

i) CLOUD OUTSOURCE STORAGE SERVICES

Application users utilize various cloud application services via AAs. TPA is reliable and independent throughout the audit functions. TPA makes regular checks on integrity and availability of delegated data at appropriate intervals. TPA able to organize, manages and maintain outsourced data and support dynamic data operations.TPA takes evidences fordisputes about inconsistency of data in terms of authentic records for all data operations.

ii) TAG GENERATION

Client uses a secret key topreprocess a fileconsists of a collection of blocks. Blocks generate a set of public verification parameters (PVPs) and Index Hash Table (IHT) stored in TPA. It transmits the file to some verification tags and CSPdelete its local copy.Signature tag of a block is generated to construct a response in terms ofTPA's challenges in the verification protocol. If the tag is unforgeable by anyone except original signer then called as secure tag. Response is verified without raw data. Block-tag pairs are stored in CSP encrypted secrets (called as PVP) are in TPA. Fragment structure is simple but file is split into sectors each block corresponds to a tag. Storage of signature tags is reduced with the increase of sectors. Structure reduces extra storage for tags improve audit performance.

iii) PERIODIC SAMPLING AUDIT AND DYNAMIC OPERATION

Periodic sampling approach to audit outsourced data audit activities are scheduled in an audit period. TPA needs to access small portions of files to perform audit in each activity detect exceptions periodically reduce sampling numbers in each audit. Index-Hash Table support dynamic data operations record the changes of file blocks generate hash value of each block in the verification process. Structure of IHT is similar to file block allocation table in file systems. Periodic sampling audit use interactive proof of retrievability. Audit for dynamic operations holds DO's secret key manipulate the outsourced data.

iv) CORRECTNESS VERIFICATION AND ERROR LOCALIZATION

Error localization is prerequisite for eliminating errors in storage systemsto identify potential threats from external attacks. Integrating correctness verification and error localization identify the misbehaving serverin the challenge-response protocol. Once inconsistency among storage is successfully detected in rely on pre-computed verification tokens to determine where the potential data error lies.

v) FILE RETRIEVAL AND ERROR RECOVERY

Whenever data corruption is detected the comparison of pre-computed tokens and received response values to guarantee the identification. User always ask servers to send back blocks of the r rows specified in the challenge and to regenerate the correct blocks by erasure correction. Less there is no way to recover corrupted blocks due to lack of redundancy even if

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

position of misbehaving servers is known. A newly recovered block is then redistributed to the misbehaving servers to maintain correctness of storage.

V. CONCLUSION AND FUTURE WORK

A construction of dynamic audit services for untrusted and outsourced storages. It presented an efficient method for periodic sampling audit to enhance the performance of TPAs and storage service providers. Our experiments showed that our solution has a small, constant amount of overhead, which minimizes computation and communication costs.Our audit service is constructed based on the techniques, fragment structure, random sampling, and index-hash table, supporting provable updates to outsourced data and timely anomaly detection. A audit system verifies the integrity with lower computation overhead and requiring less extra storage for audit metadata.

In future work of the Secured Auditing System for Cloud Data Storage With Error Corrections Guarantees has to support dynamic data operations, it is necessary for TPA to employ an IHT to record the current status of the stored files. Some existing index schemes for dynamic scenarios are insecure due to replay attack on the same Hash values.

REFERENCES

1.Yan Zhu, Gail-JoonAhn, Hongxin Hu, Stephen S. Yau, Ho G. An, Chang-Jun Hu (2013) 'Dynamic Audit Services for Outsourced Storages in Clouds'.
2. A. Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 584–597.
3. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. Of SecureComm'08, 2008, pp. 1–10.
4. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 598–609
5. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proc. of CCS'09, 2009, pp. 213–222.
6. H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90–107
7. H.-C. Hsiao, Y.-H. Lin, A. Studer, C. Studer, K.-H. Wang, H. Kikuchi, A. Perrig, H.-M.Sun, and B.-Y.Yang, "A Study of User- Friendly Hash Comparison Schemes," Proc. Ann. Computer Security Applications Conf. (ACSAC), pp. 105-114, 2009.
8. A.R. Yumerefendi and J.S. Chase, "Strong Accountability for Network Storage," Proc. Sixth USENIX Conf. File and Storage Technologies (FAST), pp. 77-92, 2007.
9.Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," Proc. 17th ACM Conf. Computer and Comm. Security, pp. 756-758, 2010
10. M. Xie, H. Wang, J. Yin, and X. Meng, "Integrity Auditing of Outsourced Data," Proc. 33rd Int'l Conf. Very Large Databases (VLDB), pp. 782-793, 2007
11. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 1-9, 2010.
12. 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, Sept./Oct. 2009
13.C.Wang, Q.Wang, K. Ren, andW. Lou, "Ensuring data storage security in cloud computing," in Proc. of IWQoS'09, July 2009, pp. 1–9
14. D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures," Proc. Advances in Cryptology (CRYPTO '04), pp. 41-55, 2004.
15. C.-P. Schnorr, "Efficient Signature Generation by Smart Cards," J. Cryptology, vol. 4, no. 3, pp. 161-174, 1991
16. D. Boneh and X. Boyen, "Short Signatures without Random Oracles and the SDH Assumption in Bilinear Groups," J. Cryptology, vol. 21, pp. 149-177, Feb. 2008.