An Efficient Secure System for Data Integrity and Replication in Cloud

Sasmita Pani[1], Surabika Hota[2], Sitanath Biswass[2]

[1]Associate professor, [2]Assistant Professor, [1,2]Dept. of CSE

[1,2]Gandhi Institute for Technology, Bhubaneshwar, India

Abstract

The cloud computing is popular for the virtually storing data because it provides the big storage space and provides the portability and mobility functions. Even if data de duplication is main advantages in security and privacy concern occur as user's confidential data are liable to both attacks insider and outsider. A convergent encryption method imposes data security while making de duplication possible. Traditional de duplication systems based on convergent encryption even though offer confidentiality but do not maintain the duplicate check on basis of differential rights. The cloud storage service (CSS) reuses total storage traction and maintenance. Hybrid cloud model is new deduplication constructions supporting authorized duplicate check. The proposed security models contain the illustration of security analysis model. as a proof of data contains the implementation framework of proposed authorized duplicate check scheme and conduct experiments using these prototypes the many de duplication methods are implemented in Hybrid Cloud system. Our proposed model is implemented for text file, pdf file, book, and image and video, it also verifies the confidentiality of private cloud.

Index Terms: Deduplication, authorized duplicate check, hybrid cloud, confidentiality, Secure auditing, Reliability, Cloud computing, Third Party Auditor.

1. Introduction

Cloud computing provides biggest virtualized recourse to user as services across the total internet while hiding the platform and implementing details. Cloud data service is the management of evergreen increasing mass of data [1]. To make data management security in cloud computing, deduplication is conventional technique. Data compression technique is used for eliminating the duplicate copies of among data in cloud storage to reduce the data duplication [2]. Integrity is simply defined as consistency. Integrity is one of the security factors which influence the cloud performance. Data integrity defines rules for writing data in a reliable manner to keep persistent data storages. There are number of models is recommended [3] and [4] to preserve integrity of data. Integrity is most important security for cloud data storages because it ensures about completeness of data also provide detail data that available data is correct easily accessible to authorized users only data is consistent and of high quality. Data security is most model in present organizations not fully take up this technology. The users do not use the data is being residing after uploading to cloud and even is handling his data. We consider those challenges that the users must deal when they use cloud computing [5].

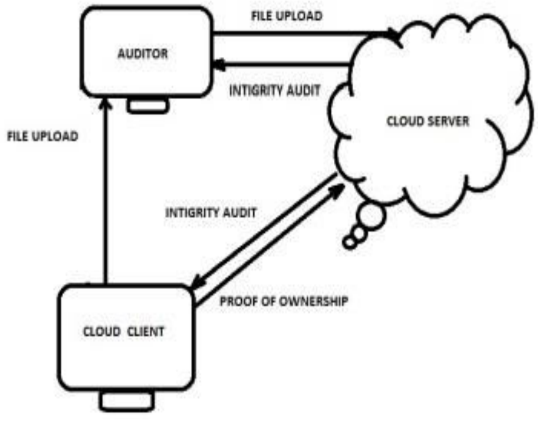

Fig.1 Secure Cloud Architecture

2. Related Work

The main goal of this work is to acquire data integrity as well as the secure data deduplication. In existing system, there was only the one server is used but in proposed system Cloud uses the multiple servers in order to load balance as well better uploading downloading speed [6]. Probabilistic queries and periodic verification as well as an optimization method of parameters of cloud audit services are implemented to provide secure access. The third-party auditor (TPA) [7] 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. The data is stored temporarily while being authorization process. Store and forward transactions processed after completing the authorization. POR [9] protocol is designed to protect a static archived file in cloud storage. Critical information stored as storage-as-service in encrypted format. It is more flexible and cost-effective storage environments. PORs lead to several possible researches in the future. The classic merles hash tree constructed for block tag authentication to achieve secure cloud storage and data dynamics. Should clients conventionally encrypt their files their savings are lost. Message locked encryption resolves this all the tension [10]. It is inherently subject to the brute force attack is recover files falling into some known set. It enables the client for storing encrypted data with an existing service that have the service perform de duplication on their behalf and yet achieves strong confidentiality guarantees [9]. Showing that encryption for the de-duplicated storage can achieve the performance and the space savings close to that of using all the storage service with plaintext data.

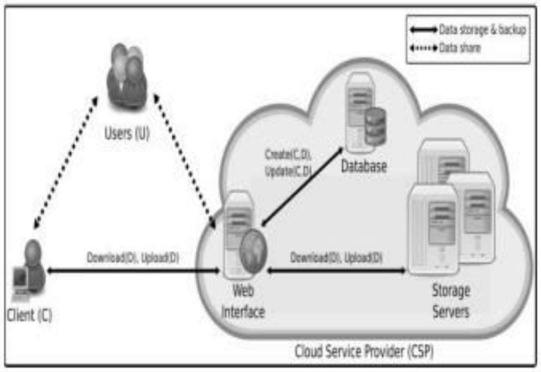

Fig. 2 Architecture of cloud data storage

3. System Model

To develop authorized data de-duplication for privacy the data security differential privileges of users in the duplicate check and conduct test bed experiments to evaluate the overhead of the prototype. De-duplication is one of most important data compression model for eliminating duplicate copies of repeating data [14].

Cloud User: A cloud user is one who needs to outsource data on public storage which acts as a public cloud in cloud computing [11].

Public Storage: Public Storage is a storage disk which permit to store the users data which contains authorization and not permit to upload the duplicate data [12].

Private Cloud: A private cloud acts as a proxy to allow both data owner and user to strongly perform duplicate check along with disparity permissions.

Auditor: Auditor is a TPA work as proficiency and capabilities where cloud users to faith assess the cloud storage service reliability on behalf of the user upon request. The user registers into the system, permissions are assigned to user according to identity given by the user at registration time means on basis of situation which access by the user [13].

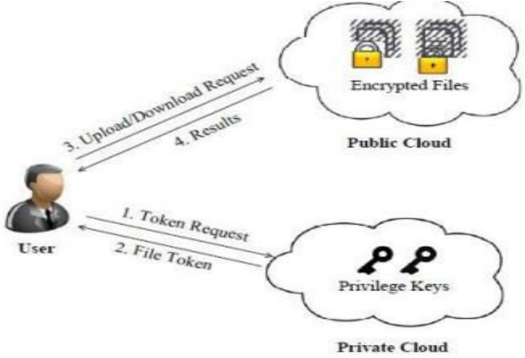

Fig. 3 Architecture of Authorized Deduplication System

4. Proposed System

User easily access the secure cloud storage model is constructed with administrator, third party auditor and cloud servers auditing model is verifying the integrity verification of cloud data storage. Administrator controls the user access of unauthorized party [15].

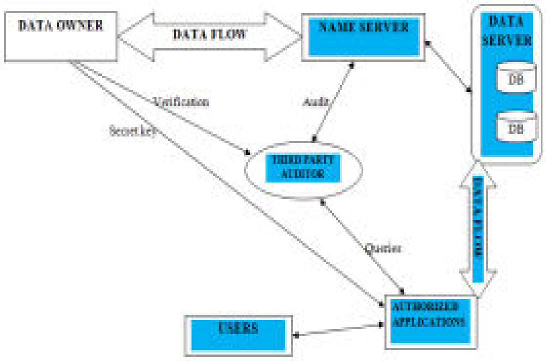

Fig. 4 System architecture of the proposed system

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 [16].

Tag Generation: The user's/clients use the secret key (sk) to pre-process a file in cloud storage. It takes access of n blocks and generates a set of public verification parameters and index hash table. User data is stored in TPA (Third party auditor) and transmits the file with some verification tags to Cloud Service Provider

Periodic Sampling Audit: TPA (Third party auditor) challenges to audit the integrity and change outsourced data stored in TPA. Audit model detects some errors in secure storage of unauthorized modification. Administrator collects all the user details within the cloud server. Verification process is constructed with insufficient proof protocol of cloud storage [17].

Audit for Dynamic Operations: Authorized application holds the secret key (sk) and it can modify the index hash table stored in TPA. User inserts the files in cloud storage with authorized access from administrator.

A. Dynamic Data Operations

Insert operation: User inserts the file in cloud storage and file is stored in Encrypted data format. Audit process audits the file in secure methods 18]

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

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

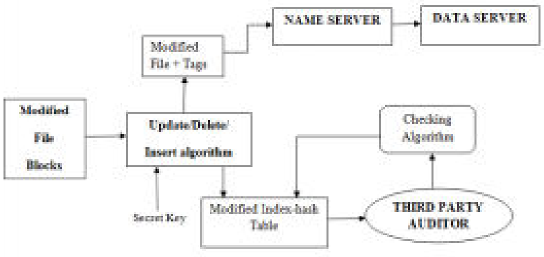

Fig. 5 Flow of dynamic data operation

Checking algorithm to tests the audit model is controlled by Administrator. The User data application takes and Update, Delete, and Insert algorithms, and then sends to TPA and CSP, respectively. It is important to security and audit process of TPA [17]. Finally, Admin gives the permission to change audit records after the confirmation message from CSP is received.

5. Algorithm

1. Take any one of the following user information. Username, password, mobile number, uploaded document name, document size.
2. Convert bit to byte conversion.
3. Byte conversion answer placed in 64*64 cells.
4. Insertion order is not unique.
5. Reorders the element and placed in outside the cell
6. Finally add the mobile number or document size to reorder element

A. Hash Table Lookup

A hash table is a data structure that is used to implement an associative array. A hash table uses hash function that computes an index into an array of slots [20]. In a well-dimensioned hash table and average cost for lookup is independent of the number of elements. Many hash tables designs access arbitrary insertions and deletions of key-value pairs which are performed at constant average cost per operation.

B. Merkle Hash Tree

A hash tree is every non-leaf node is labeled with the hash of the labels of its children nodes. Hash trees is used to verify any security data stored. Currently the main use of hash trees is to make sure that data blocks received from other peers in a peer-to-peer network is received unaltered and undamaged [21] and even to check that the other peers do not send fake blocks.

6. Result

The authorizes deduplication model used is removed duplicate copies of data in the given cloud. Proposed system implemented by using block level duplication which compare the given blocks with database, the data will be store security format and maintain security each block contain their own token, cipher text and private key. The database size will be reduced by using this technique. The prototype of proposed system is implemented use new technology. The server machine has configuration of Intel Core Duo CPU 2.4 GHz with 4GB of RAM. Heidisql used for the database storage. When user upload file, it divides into the blocks then another same file is uploaded at that time it compare with given database

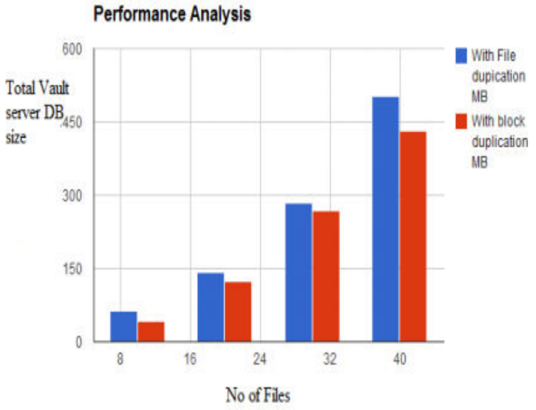

Fig. 6 Comparison between file level deduplication

7. CONCLUSION

Secure upload we can assure the user about high data security and are move data deduplication. Security analysis finding our schemes is secure in terms of insider as well as outsider attacks the proposed security model. It increased the data integrity of the cloud storage and remove the hackers to access the storage process. File insertion, File updating, File deletion is possibly used to authorized users. Cloud service users offered an audit service to audit the integrity and availability of Secure Storage Pool. Additional this will enable secure block level deduplication through introducing a Proof of Ownership protocol and preventing all the leakage of side information in data deduplication. In future, the methodology is proposed to resolve the security related model is used to endeavor on numerous security model that has been mentioned, in order to cater translucent services that can be trusted by all users.

8. FUTURE WORK

It introduces the proof of ownership protocol for element the leakage of side channel information. As compare to previous work computation time is decreased here. SecCloud+ uses the security mechanism for stored file. In simple words, it stores all files in encrypted format. Future work includes introduction of concept parallel computing, to support it multi-threading environment is useful it helps in improving the overall auditing performance

References

[1] Jin Li and Yan Kit Li ˙A Hybrid cloud approach for secure authorized de-doplication, IEEE Transaction on parallel and distributed system, vol:pp:99 2014

[2] M. Bellare, S. Keelveedhi, and T. Ristenpart. Dupless: Server aided encryption for deduplicated storage. In USENIX Security Symposium, 2013. [3] Chandinee Saraswathy K. , Keerthi D. , Padma G. "HLA Based Third Party Auditing For Secure Cloud Storage" International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1526-1532

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,”in the Proceedings of IEEE INFOCOM 2010, 2010, pp. 525–533

[5] Dharmendra S. Raghuwanshi et. al “MS2: Practical Data Privacy and Security Framework for Data at Rest in Cloud”, 2014 IEEE.

[6] Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, “Cooperative provable data possession for integrity verification in multicloud storage,” IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231–2244, 2012.

[7]. 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.

[8]. Cong Wang, Student Member, IEEE, Sherman S.M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE, “PrivacyPreserving Public Auditing For Secure Cloud Storage”.

[9] S. Keelveedhi, M. Bellare, and T. Ristenpart, Dupless: Server- aided encryption for deduplicated storage, in Pro- ceedings of the 22Nd USENIX Conference on Security, ser. SEC13. Washington, D.C.: USENIX Association, 2013, pp. 179194.

[10] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song, Remote data checking using provable data possession, ACM Trans. Inf. Syst. Secur., vol. 14, no. 1, pp. 12:112:34, 2011.

[11] M. Bellare,C. Namprempre, and G.Neven. Security proofs for identity-based identification and signature schemes. J. Cryptology, 22(1):1–61, 2009.

[12] Block-Level Deduplication with Encrypted Data Z.Wilcox-O'Hearn and B. Warner.Tahoe:In Proc. of ACM StorageSS, 2008.

[13] M. W. Storer, K. Greenan, D. D. E.Long, and E. L. Miller. Secure data deduplication. In Proc. of StorageSS, 2008.

[14] M. Bellare, C. Namprempre , and G. Neven. Security proofs for identity-based identification and signature schemes. J. Cryptology, 2009.

[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 highavailability and integrity layer for cloud storage," in Proc. of CCS'09. Chicago, IL, USA: ACM, 2009, pp. 187–198.

[19] Block-Level Deduplication with Encrypted Data Z.Wilcox-O'Hearn and B. Warner.Tahoe:In Proc. of ACM StorageSS, 2008.

[20] M. W. Storer, K. Greenan, D. D. E.Long, and E. L. Miller. Secure data deduplication. In Proc. of StorageSS, 2008.

[21] J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer. Reclaiming space from duplicate files in a serverless distributed file system. In ICDCS, pages 617–624, 2002.