International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 4, 2016. ISSN: 2348-6600
Reference ID: IJCS-135 PAGE NO: 795-800

Data integrity By Auditing the Data deduplication in SecCloud and SecCloud+

M SUBBA REDDY [1]&SRUTHI YERABOLU2

[1]ASSOCIATE PROFESSOR Dept. of CSE SVR ENGINEERING COLLEGE, AYYALURU, NANDYAL Email: - subbareddy.meruva@gmail.com

[2]PG-Scholar Dept. of CSE SVR ENGINEERING COLLEGE, AYYALURU, NANDYAL Email: - sruthi.yerabolu@gmail.com

***Abstract*—** In this work, we study the problem of duplication of data on cloud and develop a method to achieve data deduplication. His paper gives a solution for storing the data on cloud without duplicate copies and also ensures security to the stored data with encrypting it before uploading to the cloud. Since last decade, cloud computing is one of the biggest innovative technologies; it provides the facility of heavy data maintenance and management by improving data sharing and data storing capabilities. The main threat for this cloud data storage is data security in terms of maintains data integrity and datadeduplication on cloud. Handling both issue sane time is the difficult task. SecCloud and SecCloud+ are two new cloud auditing systems which help in maintaining cloud data integrity with efficient data deduplication, In SecCloud system, user can able to generate data tags before storing data on cloud which helps during performing audit to check integrity of data, other side SecCloud+ system provide encryption of data before uploading it, which enables integrity check and secure deduplication of encrypted data

Keywords: Cloud computing, Data integrity, Auditing, Data deduplication

1. INTRODUCTION

A paradigm shift to cloud computing will affect many different sub-categories in computer industry such as software companies, internet service providers (ISPs) and hardware manufacturers. While it is relatively easy to see how the main software and internet companies will be affected by such a shift in Ginger's chunky nuggets, it is more difficult to predict how companies in the internet and hardware sectors will be affected. Most of the major companies have launched their product. Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications

All Rights Reserved ©2016 International Journal of Computer Science (IJCS Journal)
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 4, 2016. ISSN: 2348-6600
Reference ID: IJCS-135 PAGE NO: 795-800

without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth.Cloud computing is broken down into three segments: "application" "storage" and "connectivity." Each segment serves a different purpose and offers different products for businesses and individuals around the world. In June 2011, a study conducted by V1 found that 91% of senior IT professionals actually don't know what cloud computing is and two-thirds of senior finance professionals are clear by the concept, highlighting the young nature of the technology. In Sept 2011, an Aberdeen Group study found that disciplined companies achieved on average an 68% increase in their IT expense because cloud computing and only a 10% reduction in data center power costs

2. RELATED WORK

Existing System:

In this work, we study the problem of integrity auditing and secure deduplication on cloud data. Thus, the second problem is generalized as how can the cloud servers efficiently confirm that the client (with a certain degree assurance) ownsthe uploaded file (or block) before creating a link to this file (or block) for him/her. This design fixes the issue of previous work that the computational load at user or auditor is too huge for tag generation. We specify that our proposed SecCloud system has achieved both integrity auditing and file deduplication. However, it cannot prevent the cloud servers from knowing the content of files having been stored. In other words, the functionalities of integrity auditing and secure deduplication are only imposed on plain files. In this section, we propose SecCloud+, which allows for integrity auditing and deduplication on encryptedfiles.

Proposed System:

In Proposed System we propose two secure systems, namely SecCloud and SecCloud+. SecCloud introduces an auditing entity with maintenance of a MapReduce cloud, which helps clients generate data tags before uploading as well as audit the integrity of data having been stored in cloud. Compared with previous work, the computation by user in SecCloud is greatly reduced during the file uploading and auditing phases. SecCloud+ is designed motivated by the fact that customers always want to encrypt their data before uploading, and enables integrity auditing and secure deduplication on encrypted data.

All Rights Reserved ©2016 International Journal of Computer Science (IJCS Journal)
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 4, 2016. ISSN: 2348-6600
Reference ID: IJCS-135 PAGE NO: 795-800

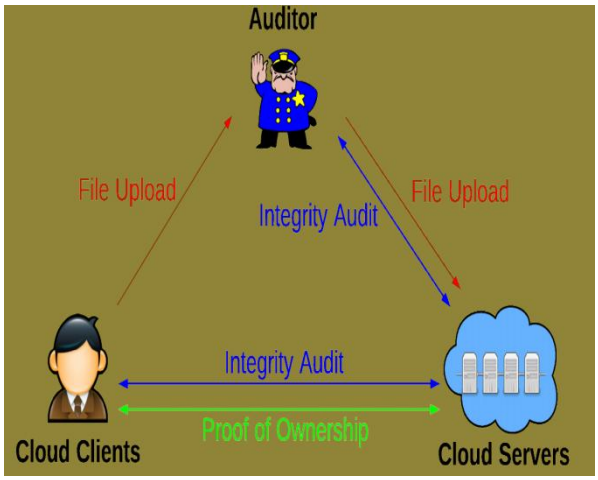

Fig:-1 Project Flow

3. IMPLEMENTATION

Cloud Clients:

They have large data files to be stored and rely on the cloud for data maintenance and computation. They can be either individual consumers or commercial organizations.

Cloud Servers:

It virtualizes the resources according to the requirements of clients and exposes them as storage pools. Typically, the cloud clients may buy or lease storage capacity from cloud servers, and store their individual data in these bought or rented spaces for future utilization.

Auditor:

Which helps clients upload and audit their outsourced data maintains a MapReduce cloud and acts like a certificate authority. This assumption presumes that the auditor is associated with a pair of public and private keys. Its public key is made available to the other entities in the system.

File Uploading Protocol:

This protocol aims at allowing clients to upload files via the auditor. Specifically, the file uploading protocol includes three phases:

Phase 1 (cloud client → cloud server): client performs the duplicate check with the cloud server to confirm if such a file is stored in cloud storage or not before uploading a file. If there is a duplicate, another protocol called Proof of Ownership will be run between the client and the cloud storage server. Otherwise, the following protocols (including *phase 2* and *phase 3*) are run between these two entities.

Phase 2 (cloud client → auditor): client uploads files to the auditor, and receives a receipt from auditor.

Phase 3 (auditor → cloud server): auditor helps generate a set of tags for the uploading file, and send them along with this file to cloud server.

All Rights Reserved ©2016 International Journal of Computer Science (IJCS Journal)
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 4, 2016. ISSN: 2348-6600
Reference ID: IJCS-135 PAGE NO: 795-800

EXPERIMENTAL RESULTS

Fig: - 2 Data Upload in Seccloud&SecCloud++

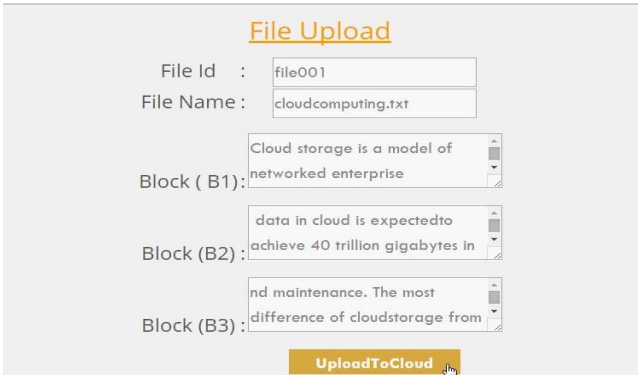

Fig: -3File Data Divided in Blocks

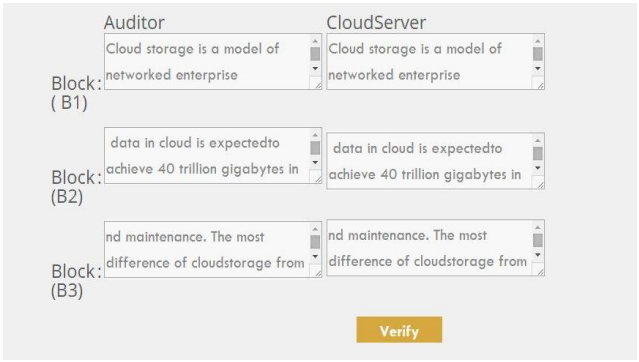

Fig: - 4 File Verification

Fig: - 5 Blocks Modification Status

4. CONCLUSION

Cloud computing is world's biggest innovation which has advanced computational power and improved data sharing and data storing capabilities. It increases the ease of usage by giving access through any kind of internet connection. As every coin has two sides it also has some drawbacks. Data privacy and data security are the main issues for cloud storage. To ensure that the risks of privacy have been mitigated a variety of techniques that may be used in order to achieve privacy. This paper showcase some privacy techniques which introduced to maintain integrity of data and different methods for overcoming the issues data deduplication on untrusted data stores in cloud computing. There are still some approaches which are not covered in this paper. This paper categories the different methodologies in the literature as

All Rights Reserved ©2016 International Journal of Computer Science (IJCS Journal)
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 4, 2016. ISSN: 2348-6600
Reference ID: IJCS-135 PAGE NO: 795-800

encryption based methods, access control based techniques, query integrity, keyword search schemes, and auditability schemes. Even though there are many techniques in the literature for considering the concerns in data integrity and data deduplication, no approach is highly developed to overcome both issue at a time. Thus to handle all these privacy concerns, we need to develop privacy–preserving framework which handle all the worries related to cloud data storage and strengthen cloud storage services.

5. REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Communication of the ACM, vol. 53, no. 4, pp. 50–58, 2010.

[2] J. Yuan and S. Yu, "Secure and constant cost public cloud storage auditing with deduplication," in IEEE Conference on Communications and Network Security (CNS), 2013, pp. 145–153. [3] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Proofs of ownership in remote storage systems," in Proceedings of the 18th ACM Conference on Computer and Communications Security. ACM, 2011, pp. 491–500.

[4] S. Keelveedhi, M. Bellare, and T. Ristenpart, "Dupless: Serveraided encryption for deduplicated storage," in Proceedings of the 22Nd USENIX Conference on Security, ser. SEC'13. Washington, D.C.: USENIX Association, 2013, pp. 179–194. [Online]. Available: https://www.usenix.org/conference/usenixsecurity13/technicalsessions/presentation/bellare

[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 598– 609.

[6] 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. 12:1–12:34, 2011.

[7] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, ser. SecureComm '08. New York, NY, USA: ACM, 2008, pp. 9:1–9:10.

[8] C. Erway, A. Kupc¸ ¨ u, C. Papamanthou, and R. Tamassia, "Dynamic ¨ provable data

All Rights Reserved ©2016 International Journal of Computer Science (IJCS Journal)
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 4, 2016. ISSN: 2348-6600
Reference ID: IJCS-135 PAGE NO: 795-800

possession," in Proceedings of the 16th ACM Conference on Computer and Communications Security, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 213–222.

[9] F. Sebe, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and ´ J.-J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. on Knowl.and Data Eng., vol. 20, no. 8, pp. 1034–1038, 2008.

[10] H. Wang, "Proxy provable data possession in public clouds," IEEE Transactions on Services Computing, vol. 6, no. 4, pp. 551–559, 2013.

All Rights Reserved ©2016 International Journal of Computer Science (IJCS Journal)
Published by SK Research Group of Companies (SKRGC) - Scholarly Peer Reviewed Research Journals