An Enhanced Multi-Layered Cryptosystem Based Secure and Authorized auditing deduplication Model in Cloud Storage System

K. Mamatha[1], D.Nandini[2], K. Raja Manohar Reddy[3]

Dept. of IT, Lakireddy Balireddy College of Engineering, Andhra Pradesh, India

***Abstract*— *As the cloud computing technology develops during the recent days, outsourcing data to cloud service for storage becomes an attractive trend, which benefits in sparing efforts on heavy data maintenance and management. Nevertheless, since the outsourced cloud storage is not fully trustworthy, it raises security concerns on how to realize data deduplication in cloud while achieving integrity auditing. In this work, we study the problem of integrity auditing and secure deduplication on cloud data. Specifically, willing achieving both data integrity and deduplication in cloud, we propose two secure systems, namely SecCloud and SecCloud. SecCloud introduces an auditing entity with maintenance of a Map Reduce cloud, which helps clients generate data tags before uploading still 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 individually fact that customers always must encrypt their data before uploading, and enables integrity auditing and secure deduplication on encrypted data.*

Keywords*—*cloud storage, data deduplication, secure auditing, proof of ownership protocol, Proof of retrievability, proof of ownership.

I. INTRODUCTION

As the cloud computing technology develops around the continue decade, outsourcing story to cloud enrollment for computerized information becomes an bright trend, which benefits in sparing efforts on chief disclosure reprieve and management. Nevertheless, as a result of the outsourced leave in the shade storage is not far trustworthy, it raises stake concerns on at which point to notice front page new de-duplication in outweigh interim achieving moral auditing. In this employment, we design the stoppage of moral auditing and win de-duplication on dwarf data. Specifically, determined achieving both data principle and de-duplication in cloud, we propose two secure systems, namely Sec-Cloud and Sec-Cloud. Sec-Cloud introduces an auditing entity by the whole of maintenance of a Map Reduce cloud, which helps clients arouse data tags once uploading as abundantly as audit the integrity of data having been collected in cloud. Compared mutually previous function, the computation by addict in Sec-Cloud is profoundly reduced around the file uploading and auditing phases. Sec-Cloud is designed motivated by the rundown that customers eternally want to encrypt their data earlier uploading, and enables integrity auditing and achieve de-duplication on encrypted data.

Cloud storage systems are becoming increasingly popular. A promising technology that keeps their cost down is deduplication.More specifically, an attacker who knows the hash signature of a file can convince the storage service that it owns that file; hence the server lets the attacker download the entire file. .Data security is also challenge in the cloud server.

II. RELATED WORK

The definition of demonstrable knowledge possession (PDP) was introduced by Ateniese et al. [5][6] for reassuring that the cloud servers possess the target files while not retrieving or downloading the total knowledge. Basically, PDP may be a probabilistic proof protocol by sampling a random set of blocks and asking the servers to prove that they precisely possess these blocks, and also the admirer solely maintaining a little quantity of information is in a position to perform the integrity checking. when Ateniese et al.'s proposal [5], many works involved directed understand PDP on dynamic scenario: Ateniese et al. [7] planned a dynamic PDP schema however while not insertion operation; Erway et al. [8] improved Ateniese et al.'s work [7] and supported insertion by introducing documented flip table; an identical work has additionally been contributed in [9]. However, these proposals [5][7][8][9] receive the machine overhead for tag generation at the consumer. To mend this issue, Wang et al. [10] planned proxy PDP publicly clouds. Zhu et al. [11] planned the cooperative PDP in multi-cloud storage. Another line of labor supporting integrity auditing is proof of retrievability

(POR) [12]. Compared with PDP, POR not just assures the cloud servers possess the target files, however additionally guarantees their full recovery. In [12], purchasers apply erasure codes and generate authenticators for every block for verifiability and retrievability. So aside realize economical knowledge dynamics, Wang et al. [13] improved the POR model by manipulating languages Merkle hash tree construction for block tag authentication. Xu and Yangtze River [14] planned to enhance the POR schema in [12] with polynomial commitment for reducing communication value. Stefanov et al. [15] proposed a POR protocol over authenticated file system if frequent changes. Azraoui et al. [16] combined the privacy-preserving word search algorithm with the insertion in data segments of randomly generated short bit sequences, and developed a new POR protocol. Li et al. [17] considered a new cloud storage architecture with two independent cloud servers for integrity auditing to reduce the computation load at client side. Recently, Li et al. [18] utilized the key-disperse paradigm to fix the issue of a significant number of convergent compute convergent encryption. B. Secure Deduplication Deduplication is a technique where the server stores only a single copy of each file, nevertheless how many clients asked to store that file, such that the disk space of cloud servers likewise network bandwidth are saved. However, trivial client side deduplication accelerate the leakage of side channel information. For example, a server telling a client full need not send the file reveals that that client has the exact same file, which perchance sensitive information in some case. In order to restrict the leakage of side channel information, Halevi et al. [3] introduced the proof of ownership protocol which lets a client efficiently prove to a server that that the client exactly holds this file. Several proof of ownership protocols based on the Merkle hash tree are proposed [3] to enable secure client-side deduplication. Pietro and Sorniotti [19] proposed an efficient proof of ownership scheme by choosing the projection of a file onto some randomly selected bit-positions as the file proof. Another career for secure deduplication dig the confidentiality of DE duplicated data and considers to make deduplication on encrypted data. Ng et al. [20] firstly introduced the private data deduplication as a complement of public data deduplication protocols of Halevi et al. [3]. Convergent encryption [21] is a promising cryptographic primitive for ensuring data privacy in deduplication. Bellare et al. [22] formalized this primitive as message-locked encryption, and explored its application in space-efficient secure outsourced storage. Abadi et al. [23] further strengthened Bellare et AL’s security definitions [22] by considering plaintext distributions so anticipate the public parameters of the schemas. Regarding the practical implementation of convergent encryption for securing deduplication, Keelveedhi et al. [4] designed the Dupless system anywhere clients encrypt under file-based keys derived from a key server via an oblivious pseudorandom function protocol. As stated before, all the works illustrated above considers either integrity auditing or deduplication, while in this paper, we attempt to solve both problems simultaneously. Additionally, it's worth noting that our work is additionally distinguished with [2] that audits cloud knowledge with deduplication, as we have a tendency to additionally envisage to 1) source the computation of tag generation, 2) audit and DE duplicate encrypted knowledge within the planned protocols.

III. SYSTEM MODEL

1. **User**: It is nothing but cloud clientswhen a client wants to store a huge data they rely on cloud for maintenance and computation
2. **Cloud server**: It virtualizes theresources based on the client’s requirements and expose them as storage pools
3. **Auditors:** Which helps clients to upload and maintains their data and acts like a certificate authority. Auditor is associated with pair of public and private keys and public key is made available.

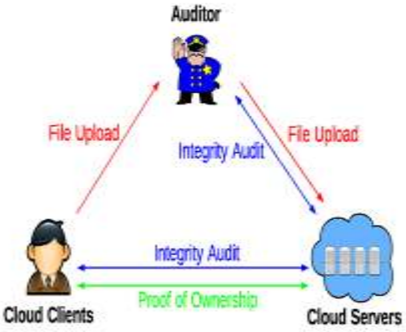

Fig: System architecture

IV. PROPOSED WORK

In this project, aiming at achieving data integrity and deduplication in cloud, 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 integrity of data having been stored in cloud.Besides supporting integrity auditing and secure deduplication, SecCloud+ enables the guarantee of file confidentiality.We propose a method of directly auditing integrity on encrypted data.

V. PERORMANCE EVALUTION

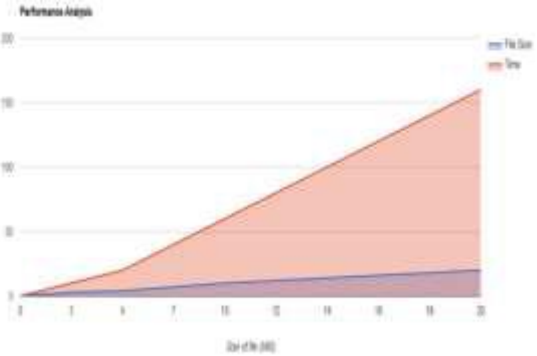

Fig: Performance Analysis

In this performance analysis graph we show the relationship between the files and their time to upload in server. In this above graph, we consider the size of the file on x-axis and time on y-axis from 0 to infinity these values will change dynamically based on the time. If the file size is small the uploading time is less. If the file size is huge then it takes more amount of time to upload file into server. Based on the size of the files only the uploading time will be depended.

VI. CONCLUSION

We are focusing to achieve both data integrity and data de-duplication in cloud, we propose SecCloud and SecCloud+. SecCloud introduce an auditing entity with maintenance of a Map Reduce cloud, which helps the clients to generate data tags before uploading and audit the integrity of data having been stored in cloud. In addition, SecCloud enables secure de-duplication by introducing a Proof of Ownership protocol (POP) and preventing the leakage of side channel information in de-duplication. We compared with the existing work; the computation by user in SecCloud is greatly reduced during the file uploading and auditing phases. Sec - Cloud+ is an advanced construction motivated by the fact that customers always want their data to be encrypted before uploading, and allows for integrity auditing as well as secure de-duplication directly on encrypted data.

REFERENCES

[1] Imai, Shigeru, Thomas Chestna, and Carlos A. Varela. "Elastic scalable cloud computing using application-level migration." *Utility and Cloud Computing (UCC), 2012 IEEE Fifth International Conference on*. IEEE, 2012.

[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: Server aided encryption for DE duplicated storage,” in Proceedings of the 22Nd USENIX Conference on Security, ser. SEC’13. Washington, D.C.: USENIXAssociation,2013,pp.179194.[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 checkingusing 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 Networks, ser. SecureComm ’08. New York, NY, USA: ACM, 2008, pp. 9:1–9:10. 8. C. Erway, A. K¨upc ̧¨u, C. Papamanthou, and R.Tamassia, “Dynamic provable data 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.

[8] F. Seb ́e, J. Domingo-Ferrer, A. Martinez-Balleste, Y.Deswarte, and J.-J. Quisquater, “Efficient remote data © 2015, IRJET ISO 9001:2008 Certified Journal Page 653 International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 02 Issue: 09 | Dec-2015 www.irjet.net p-ISSN: 2395-0072.

[9] J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou, “Secure deduplication with efficient and reliable convergent key management,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 6, pp. 1615–1625, June2014.