International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 3, March-April 2022 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Hybrid Cloud Approach with Security and Data Deduplication

R Amrutha[1], Prof Dr. Murugan R[2]

[1]Research Scholar, [2]Associate Professor,
[1,2]School of Computer Science and Information Technology,
Jain (deemed to be University), Bangalore, Karnataka, India

ABSTRACT

Data Deduplication technique is used to protect the confidentiality of sensitive data while supporting deduplication, the convergent encryption technique has been proposed to encrypt the data before outsourcing for better data security, this approach makes the first attempt to formally address the problem of authorized datadeduplication. Different from traditional deduplication systems, the differential privileges of users are further considered in duplicate check besides the data itself. Several new deduplication constructions are proposed supporting authorized duplicate check in a hybrid cloud architecture. Security analysis demonstrates that this scheme is secure in terms of the definitions specified in the proposedsecurity model.

How to cite this paper: R Amrutha | Prof Dr. Murugan R "Hybrid Cloud Approach with Security and Data Deduplication" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-3, April 2022, pp.436-437, URL: www.ijtsrd.com/papers/ijtsrd49521.pdf

IJTSRD49521

1. INTRODUCTION

Data deduplication is a specialized data compression technique for eliminating duplicate copies of repeating data in storage. The technique is used to improve storage utilization and can also be applied to network data transfers to reduce the number of bytes that must be sent. Instead of keeping multiple data copies with the same content, deduplication eliminates redundant data by keeping only one physical copy and referring other redundant data to that copy. Deduplication can take place at either the file level or the block level. For file level deduplication, it eliminates duplicate copies of the same file. Deduplication can also take place at the block level, which eliminates duplicate blocks of data that occur in non-identical files.

2. LITERATURE SERVEY

"Survey on Authorized Data Deduplication System using Cryptographic and Access Control Techniques" Santoshi S Patil, Samprati T, Asst. Prof. Swetha K S,published in 2014

Ever increasing volume of back up data in cloud storage may be a vital challenge back up windows are shrinking due to growth of information. We use the concept of deduplicate. Deduplication means duplicate data is eliminated a pointer is created to reference a data that is backed up. Deduplication can take place at file level, in this it detects redundant data within and across files or at the block level, in this it removes redundant copies of identical files

3. EXISTINGSYSTEM

Traditional encryption, while providing data confidentiality, is incompatible with data deduplication. Specifically, traditional encryption requires different users to encrypt their data with their own keys. Convergent encryption has been proposed to enforce data confidentiality while making deduplication feasible. It encrypts/decrypts a data copy with a convergent key, which is obtained by computing the cryptographic hash value of the content of the data copy. After key generation and data encryption, users retain the keys and send the cipher text to the cloud. Identical data copies will generate the same convergent key and hence the same cipher text.

3.1. Disadvantages of the existing system

- Existing deduplication systems cannot support differential authorization duplicate check, which is important in many applications.
- Traditional deduplication systems based on convergent encryption, although providing confidentiality to some extent, do not support the duplicate check with differential privileges.

4. PROPOSEDSYSTEM

Aiming at efficiently solving the problem of deduplication with differential privileges in cloud computing, a hybrid cloud architecture is considered consisting of a public cloud and a private cloud. Private cloud is involved as a proxy to allow data owner/users to securely perform duplicate check with differential privileges. Such an architecture is practical and has attracted much attention from researchers. The data owners only outsource their data storage by utilizing public cloud while the data operation is managed in private cloud. A new deduplication system supporting differential duplicate check is proposed under this hybrid cloud architecture where the S-CSP resides in the public cloud. The user is only allowed to perform the duplicate check for files marked with the corresponding privileges.

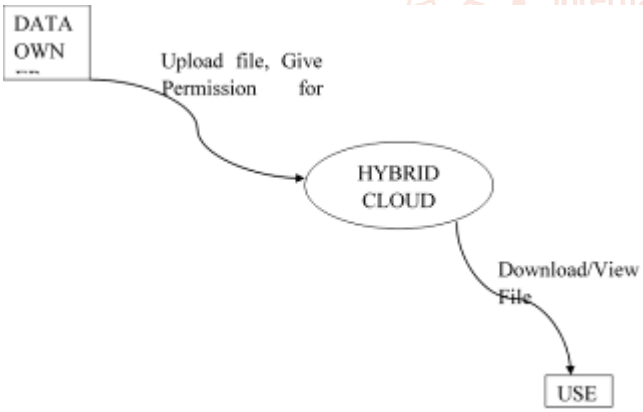

Fig 4.1

5. CONCLUSION

In this project, the notion of authorized data deduplication was proposed to protect the data security by including differential privileges of users in the duplicate check. We also presented several new deduplication constructions supporting authorized duplicate check in hybrid cloud architecture, in which the duplicate-check tokens of files are generated by the private cloud server with private keys. Security analysis demonstrates that our schemes are secure in terms of insider and outsider attacks specified in the proposed security model. As a proof of concept, we implemented a prototype of our proposed authorized duplicate check scheme and con-duct testbed experiments on our prototype.

6. ACKNOWLEDGEMENT

I should convey my real tendency and obligation to Dr M N Nachappa and Dr. Murugan R undertaking facilitators for their effective steerage and consistent inspirations all through my assessment work. Their ideal bearing, absolute co-action and second discernment have made my work Gainful.

7. REFERENCES

[1] P. Anderson and L. Zhang. Fast and secure laptop backups with encrypted de duplication. In *Proc. of USENIX LISA*, 2010.

[2] M. Bellare, S. Keelveedhi, and T. Ristenpart. Dupless: Serveraided encryption for deduplicated storage. In *USENIX Security Symposium*, 2013.

[3] M. Bellare, S. Keelveedhi, and T. Ristenpart. Message-locked encryption and secure deduplication. In *EUROCRYPT*, pages 296–312, 2013.

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

[5] M. Bellare and A. Palacio. Gq and schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks. In *CRYPTO*, pages 162–177, 2002.

[6] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider. Twin clouds: An architecture for secure cloud computing. In *Workshopon Cryptography and Security in Clouds (WCSC 2011)*, 2011.

[7] 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.

[8] D. Ferraiolo and R. Kuhn. Role-based access controls. In *15th NIST-NCSC National Computer SecurityConf.*1992.

[9] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-based access control models. *IEEE Computer*, 29:38–47, Feb 1996.

[10] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg. Proofs of ownership in remote storage systems. In Y. Chen, G. Danezis, and V. Shmatikov, editors, *ACM Conference on Computer and Communications Security*, pages 491–500. ACM, 2011