ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 2, February 2015*

5th International Conference in Magna on Emerging Engineering Trends 2015 [ICMEET 2015]

On 27th & 28th February, 2015

Organized by

Department of Mechanical Engineering, Magna College of Engineering, Chennai-600055, India.

Enhanced In-Line Data Deduplication and Secure Authorization in Hybrid Cloud

G.Kumaresan, L.Maria Michael Visuwasam

PG Scholar, Department of CSE, Velammal Institute of Technology, Panchetti, Chennai, India

Assistant Professor, Department of CSE, Velammal Institute of Technology, Panchetti, Chennai, India

ABSTRACT: Data deduplication is one of the hottest technologies in storage right now because it enables companies to save a lot of money on storage costs to store the data and on the bandwidth costs to move the data when replicating it offsite for DR. This is great news for cloud providers, because if you store less, you need less hardware. Data deduplication is one of important data compression techniques for eliminating duplicate copies of repeating data, and has been widely used in cloud storage to reduce the amount of storage space and save bandwidth. To protect the confidentiality of sensitive data while supporting deduplication, the convergent encryption technique has been proposed to encrypt the data before outsourcing. Different from traditional deduplication systems, the differential privileges of users are further considered in duplicate check besides the data itself. Whenever the cloud users upload a file to server. While sending files if it is duplicating the server will popup it is duplication message. This access is done in private cloud key generation, the deduplicate checker system will check the file names, file format, file content and file capacity and it will compare whether it is same or matching the uploading file from the exiting file in cloud server. The stored files should be encrypted after uploaded to the cloud server and are decrypted upon the client's request. Only public users need the key for decryption while the private user does not. The encryption algorithm provides data confidentiality and authentication to the cloud server.

KEYWORDS: Deduplication, authorized duplicate check, confidentiality, and hybrid cloud

I. INTRODUCTION

Cloud computing provides seemingly unlimited "virtualized" resources to users as services across the whole Internet, while it will hide the platform and implement the details. In today cloud service providers offer both highly available storage and massively parallel computing resources at relatively low costs. Cloud computing becomes prevalent and an increasing amount of data is being stored in the cloud and shared by users with specified privileges, which define the access rights for the storage data. One critical challenge of cloud storage services is the management of the ever-increasing volume of data. To make the data management scalable in cloud computing, deduplication it have been known as a technique and has attracted more and more attention recently used. The data deduplication is a specialized data compression technique for eliminating duplicate copies of repeating data's are stored. 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 the multiple data copies with the same content, which the deduplication eliminates redundant data by keeping only one physical copy and referring other redundant data to that copy. The Deduplication can take place at either the file level or at the block level. The file level deduplication, it eliminates duplicate copies of the same file. The deduplication can also take place at the block level, which eliminates the duplicate blocks of data that occur in non-identical files.

II. RELATED WORK

In this paper, aiming at efficiently solving the problem of deduplication with differential privileges in cloud computing, we consider it as a hybrid cloud architecture consisting of a public cloud and a private cloud. Unlike the existing data

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 2, February 2015

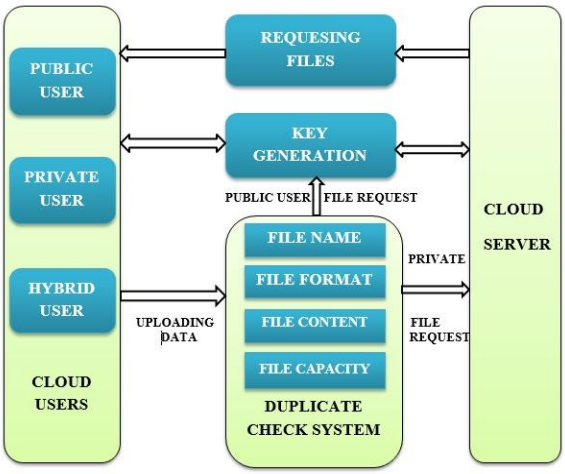
5th International Conference in Magna on Emerging Engineering Trends 2015 [ICMEET 2015]

On 27th & 28th February, 2015

Organized by

Department of Mechanical Engineering, Magna College of Engineering, Chennai-600055, India.

deduplication systems, the private cloud computing is involved in proxy to allow data owner/users to securely perform duplicate check with differential privileges.



III. CLOUD ARCHITECTURE

Such architecture is practical and has attracted much attention from the researchers. The data owners are the only outsource to 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 users are only allowed to perform the duplicate check for files marked with the corresponding privileges. Furthermore, we enhance our systems security more. Specifically, we propose at present an advanced scheme to support stronger security by encrypting the file with differential privilege keys. In this way, the users without corresponding privileges we cannot perform the duplicate check.Finally, we implement a prototype of the proposed authorized duplicate check and conduct testbed experiments to evaluate the overhead of the prototype. We show that is the overhead is minimal compared to the normal convergent encryption and file upload operations.

IV. EXISTING SYSTEM

Data deduplication is one of important data compression techniques for eliminating duplicate copies of repeating data's and it has been widely used in cloud storage to reduce the amount of storage space and save bandwidth. We protect the confidentiality of sensitive data while supporting deduplication, the cloud computing provides seemingly unlimited "virtualized" resources to users as services across the whole Internet, while it will hide platform and implement the details. In today's cloud service providers offer both the highly available storage and massively parallel computing resources at relatively low costs. The cloud computing becomes prevalent and an increasing amount of data is being stored in the cloud and shared by users with specified privileges, which define the access rights for the storage data. By using this existing system, we have similar disadvantage is one critical challenge of cloud storage services is the management of the ever-increasing volume of data.

V. PROPOSED SYSTEM

The convergent encryption technique has been proposed to encrypt the data before the outsourcing. The better protect data security wise, in this paper makes the first attempt to formally address the problem of authorized data deduplication. It is different from traditional deduplication systems, in this differential privileges of users are further considered it as duplicate check besides the data itself. We present several new deduplication constructions supporting authorized duplicate check in hybrid cloud architecture. Security analysis demonstrates that our scheme is to secure in

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 2, February 2015

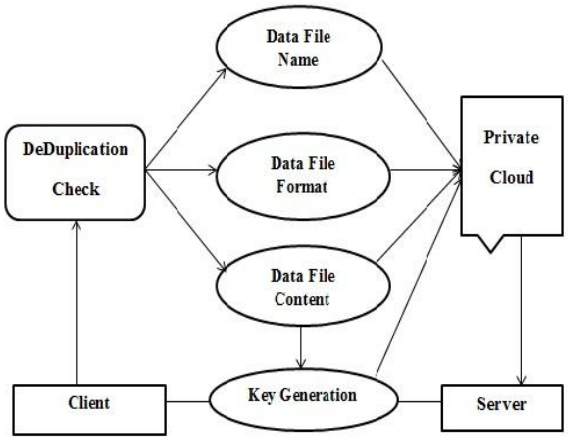
5th International Conference in Magna on Emerging Engineering Trends 2015 [ICMEET 2015]

On 27th & 28th February, 2015

Organized by

Department of Mechanical Engineering, Magna College of Engineering, Chennai-600055, India.

terms of the definitions specified in the proposed security model. The concept, we implement the prototype of our proposed authorized duplicate check scheme and conduct test bed experiments using our prototype. The proposed system is authorized to duplicate check scheme incurs minimal overhead compared to normal operations.



In proposed system, we implemented advanced technique by using this advantage is the users have to prove that the data which he wants to upload or download is its own data. A user derives a convergent key from each original data copy and encrypts the data copy with the convergent key.

VI. MODULES

USER MODULE

In this module, the users are having authentication and security to access the detail which is presented in the ontology system. Before we are accessing or searching the details user should have the account in that otherwise they should register first.

SECURE DEDUPLICATION SYSTEM

To support authorized deduplication, the tagging of a file will be determined by the file and the privilege. The difference with traditional notation of tag, we call it file token instead. To support authorized access, a secret key will be bounded with a privilege p to generate a file token. As a result, if a file has been uploaded by a user with a duplicate token, then a duplicate check sent from another user will be successful if and only if he also has the file and privilege. Such a token generation function could be easily implemented a cryptographic hash function.

SECURITY OF DUPLICATE CHECK TOKEN

We consider several types of privacy we need to protect, that is, i) unforgeability of duplicate check token: There are two types of adversaries they are external adversary and internal adversary. The external adversary can be viewed as an internal adversary without any privilege. If a user has privilege, it requires that the adversary cannot forge and output a valid duplicate token with any other privilege on any file, does not match. Furthermore, it requires that if the adversary does not make a request of token with its own privilege from private cloud server, it cannot forge and output a valid duplicate token with privilege on any file that has been queried.

ENCRYPTION KEY

Once the key request is received, the sender can send the key or he can decline it. This key and request id which was generated at the time of sending key request the receiver can decrypt the message.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 2, February 2015

5th International Conference in Magna on Emerging Engineering Trends 2015 [ICMEET 2015]

On 27th & 28th February, 2015

Organized by

Department of Mechanical Engineering, Magna College of Engineering, Chennai-600055, India.

COMPARING FILE, FILE FORMAT, FILE CONTENT AND FILE CAPACITY

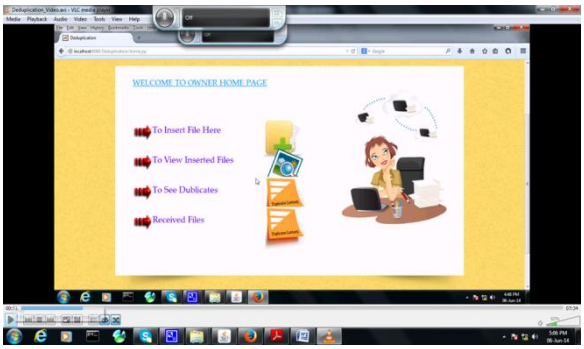
In this type we are comparing the file names whether it is same name or not. If it is same name as saved in cloud, the server will send a notification as tick mark. Comparing the file format whether it is same file format or not. If it is same file format as saved in cloud, the server will send a notification as tick mark. Comparing the file content whether it is same content or not. If it is same content as saved in cloud, the server will send a notification as tick mark. Comparing the file capacity whether it is same capacity or not. According to the comparing file capacity each format as different capacity so the server will notify the wrong mark.

VII. SIMULATION OUTPUT

REGISTRATION PAGE

LOGIN PAGE

HOME PAGE



ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 2, February 2015*

5th International Conference in Magna on Emerging Engineering Trends 2015 [ICMEET 2015]

On 27th & 28th February, 2015

Organized by

Department of Mechanical Engineering, Magna College of Engineering, Chennai-600055, India.

INSERT FILE PAGE

VIEW FILE PAGE

SEND FILE IN CLOUD SYSTEM

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 2, February 2015

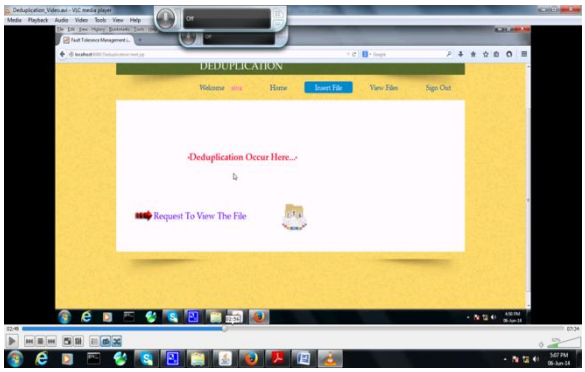
5th International Conference in Magna on Emerging Engineering Trends 2015 [ICMEET 2015]

On 27th & 28th February, 2015

Organized by

Department of Mechanical Engineering, Magna College of Engineering, Chennai-600055, India.

DEDUPLICATION SENDING REQUEST



VIII. CONCLUSION

In this project, the notion of authorized data deduplication was proposed to protect the data security by including differential privileges of users are the duplicate check. We presented several new deduplication constructions supporting authorized duplicate check in hybrid cloud architecture, in which the duplicated check tokens of files are generated by the private cloud server with private keys. The security analysis demonstrates that our schemes will be secure in terms of insider and outsider attacks specified in the proposed security model. To protect the genuine data, increased the accuracy of data duplicates check, effective hardware capacity utilization by using enhanced techniques, algorithms. RSA algorithm is used which increases the security in hybrid cloud. We proposed system is authorize the duplicate check scheme incurs minimal overhead compared to convergent encryption and network transfer.

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: Serveraidedencryption for deduplicated storage. In USENIX SecuritySymposium, 2013.
[3] 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.
[4] 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.
[5] J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer.Reclaiming space from duplicate files in a server less distributed file system. In *ICDCS*, pages 617–624, 2002.
[6] D. Ferraiolo and R. Kuhn. Role-based access controls. In *15thNIST-NCSC National Computer Security Conf.*, 1992.
[7] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg. Proofs ofownership in remote storage systems. In Y. Chen, G. Danezis,and V. Shmatikov, editors, *ACM Conference on Computer andCommunications Security*, pages 491–500. ACM, 2011.
[8] J. Li, X. Chen, M. Li, J. Li, P. Lee, andW. Lou. Secure deduplicationwith efficient and reliable convergent key management. In *IEEETransactions on Parallel and Distributed Systems*, 2013.
[9] C. Ng and P. Lee. Revdedup: A reverse deduplication storage system optimized for reads to latest backups. In *Proc. Of APSYS*, Apr 2013.
[10] R. D. Pietro and A. Sorniotti. Boosting efficiency and security in proof of ownership for deduplication. In H. Y. Youm and Y. Won, editors, *ACM Symposium on Information, Computer and Communications Security, pages 81–82. ACM, 2012.*
[11] A. Rahumed, H. C. H. Chen, Y. Tang, P. P. C. Lee, and J. C. S. Lui. A secure cloud backup system with assured deletion and version control. In *3rd International Workshop on Security in Cloud Computing, 2011*