International Journal of Science Engineering and Advance Technology

A Secure and authorized Duplication model in Cloud Using multi-layered cryptosystem based

Meesala Venkata Nooka Raju [1], K.LakshmiPriya [2]
[1]PG Scholar, Pydah College of Engineering, Kakinada, AP, India, E-mail: raju.meesala1256@gmail.com.
[2]Assistant Professor, Pydah College of Engineering, Kakinada, AP, India.

Abstract—the present a scheme that permits a more fine-grained trade-off. The intuition is that outsourced data may require different levels of the protection, depending on how to popular it is: content shared by many users, such as popular song or video, arguably requires less protection than a personal document, the copy of a payslip or the draft of an un submitted scientific paper. Unfortunately, semantically secure encryption schemes render various cost-effective storage optimization techniques, such as the data de duplication, ineffective. We present a novel idea that differentiates data according to their popularity. Based on this idea, we design an encryption scheme that the guarantees semantic security for the unpopular data and provides weaker security and better storage and bandwidth benefits for popular data

Key words: De duplication, authorized duplicate check, confidentiality, hybrid cloud

I. Introduction

In this paper, aiming at efficiently solving the problem of Deduplication with differential privileges in cloud computing, we consider a hybrid cloud architecture consisting of a public cloud and a private cloud. Unlike existing data deduplication systems, the private cloud is involved as a proxy to allow data owner/users to securely perform duplicate check with differential privileges. A new de duplication system supporting differential duplicate check is proposed under this hybrid cloud architecture where the S-CSP resides in the public cloud. Such 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. The user is only allowed to perform the duplicate check for files marked with the corresponding privileges. Further more, we enhance our system in security. Specifically, we present an advanced scheme to support stronger security by encrypting the file with differential privilege keys. In this way, the users without corresponding privileges cannot perform the duplicate check. Further more, such unauthorized users cannot decrypt the cipher text even collude with the S-CSP. Security analysis demonstrates that our system is secure in terms of the definitions specified in the proposed security model. 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 the overhead is minimal compared to the normal convergent encryption and file upload operations.

II. System Analysis

Existing System:

- Data deduplication systems, the private cloud is involved as a proxy to allow data owner/users to securely perform duplicate check with differential privileges.
- Such 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.

Disadvantages Of Existing System:

- Traditional encryption, while providing data confidentiality, is incompatible with data deduplication.
- Identical data copies of different users will lead to different cipher texts, making deduplication impossible.

Proposed System:

In this paper, we enhance our system in security. Specifically, we present an advanced scheme to support stronger security by encrypting the file with differential privilege keys. Security analysis demonstrates that our system is secure in terms of the definitions specified in the proposed security model.

Advantages Of Proposed System:

- The user is only allowed to perform the duplicate check for files marked with the corresponding privileges.
- We present an advanced scheme to support stronger security by encrypting the file with differential privilege keys.
- Reduce the storage size of the tags for integrity check. To enhance the security of deduplication and protect the data confidentiality,

II.Implementation

Modules:-

- Cloud Service Provider
- Data Users Module
- Private Cloud Module
- Secure De duplication System

Modules Descripton:-

Cloud Service Provider

- ✓ In this module, we develop Cloud Service Provider module. This is an entity that provides a data storage service in public cloud.
- ✓ The S-CSP provides the data outsourcing service and stores data on behalf of the users.
- ✓ To reduce the storage cost, the S-CSP eliminates the storage of redundant data via de duplication and keeps only unique data.
- ✓ In this paper, we assume that S-CSP is always online and has abundant storage capacity and computation power.

Data Users Module

- ✓ A user is an entity that wants to outsource data storage to the S-CSP and access the data later.
- ✓ In a storage system supporting de duplication, the user only uploads unique data but does not upload any duplicate data to save the upload bandwidth, which may be owned by the same user or different users.
- ✓ In the authorized de duplication system, each user is issued a set of privileges in the setup of the system. Each file is protected with the convergent encryption key and privilege keys to realize the authorized de duplication with differential privileges.

Private Cloud Module

- ✓ Compared with the traditional de duplication architecture in cloud computing, this is a new entity introduced for facilitating user's secure usage of cloud service.
- ✓ Specifically, since the computing resources at data user/owner side are restricted and the public cloud is not fully trusted in practice, private cloud is able to provide data user/owner with an execution environment and infrastructure working as an interface between user and the public cloud.
- ✓ The private keys for the privileges are managed by the private cloud, who answers the file token requests from the users. The interface offered by the private cloud allows user to submit files and queries to be securely stored and computed respectively.

Secure De duplication System

- ✓ We consider several types of privacy we need protect, that is, i) UN forge ability of duplicate-check token: There are two types of adversaries, that is, external adversary and internal adversary.
- ✓ As shown below, the external adversary can be viewed as an internal adversary without any privilege.
- ✓ If a user has privilege p, it requires that the adversary cannot forge and output a valid duplicate token with any other privilege p' on any file F, where p does not match p'. Furthermore, it also 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 p on any F that has been queried.

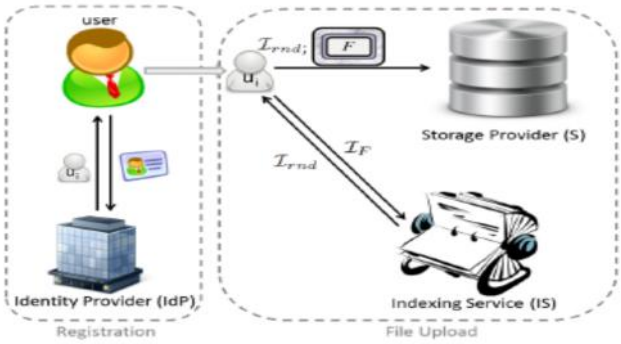

Fig 1: system architecture

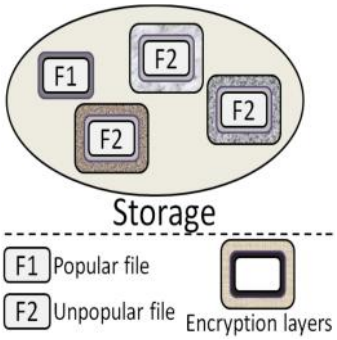

Fig: 2 Proposed multi-layered scheme

III.System Model

3.1 Hybrid Architecture for Secure Deduplication

At a high level, our setting of interest is an enterprise network, consisting of a group of affiliated clients (for example, employees of a company) who will use the S-CSP and store data with deduplication technique. In this setting, deduplication can be frequently used in these settings for data backup and disaster recovery applications while greatly reducing storage space. Such systems are widespread and are often more suitable to user file backup and synchronization applications than richer storage abstractions.

• *Private Cloud.* Compared with the traditional deduplication architecture in cloud computing, this is a new entity introduced for facilitating user's secure usage of cloud service. Specifically, since the computing resources at data user/owner side are restricted and the public cloud is not fully trusted in practice, private cloud is able to provide data user/owner with an execution environment and infrastructure working as an interface between user and the public cloud. The private keys for the privileges are managed by the private cloud, who answers the file token requests from the users. The interface offered by the private cloud allows user to submit files and queries to be securely stored and computed respectively.

Notice that this is a novel architecture for data deduplication in cloud computing, which consists of a twin clouds (i.e.,

the public cloud and the private cloud).Actually, this hybrid cloud setting has attracted more and more attention recently. For example, an enterprise might use a public cloud service, such as Amazon S3, for archived data, but continue to maintain in-house storage for operational customer data. Alternatively, the trusted private cloud could be a cluster of virtualized cryptographic co-processors, which are offered as a service by a third party and provide the necessary hardware based security features to implement a remote execution environment trusted by the users.

3.2 Adversary Model

Typically, we assume that the public cloud and private cloud are both "honest-but-curious". Specifically they will follow our proposed protocol, but try to find out as much secret information as possible based on their possessions. Users would try to access data either within or out of the scopes of their privileges. In this paper, we suppose that all the files are sensitive and needed to be fully protected against both public cloud and private cloud. Under the assumption, two kinds of adversaries are considered, that is, 1)external adversaries which aim to extract secret information as much as possible from both public cloud and private cloud; 2) internal adversaries who aim to obtain more information on the file from the public cloud and duplicate-check token information from the private cloud outside of their scopes. Such adversaries may include S-CSP, private cloud server and authorized users. The detailed security definitions against these adversaries are discussed below and in Section 5, where attacks launched by external adversaries are viewed as special attacks from internal adversaries.

3.3 Design Goals

In this paper, we address the problem of privacy preserving deduplication in cloud computing and propose a new deduplication system supporting for

• **Differential Authorization**. Each authorized user is able to get his/her individual token of his file to perform duplicate check based on his privileges. Under this assumption, any user cannot generate a token for duplicate check out of his privileges or with out the aid from the private cloud server.

• **Authorized Duplicate Check**. Authorized user is able to use his/her individual private keys to generate query for certain file and the privileges he/she owned with the help of private cloud, while the public cloud performs duplicate check directly and tells the user if there is any duplicate. The security requirements considered in this paper lie in two folds, including the security of file token and security of data files. For the security of file token, two aspects are defined as UN forge ability and in distinguish ability of file token. The details are given below.

• *Unforgeability of file token/duplicate-check token.* Unauthorized users without appropriate privileges or fileshould be prevented from getting or generating the file tokens for duplicate check of any file stored at the S-CSP. The users are not allowed to collude with the public cloud server to break the UN forge ability of file tokens. In our system, the S-CSP is honestbut curious and will honestly perform the duplicatecheck upon receiving the duplicate request from users. The duplicate check token of users should be issued from the private cloud server in our scheme.

• *Indistinguishability of file token/duplicate-check token.* It requires that any user without querying the private cloud server for some file token, he cannot get any useful information from the token, which includes the file information or the privilege information.

• *Data Confidentiality.* Unauthorized users without appropriate privileges or files, including the S-CSP and the private cloud server, should be prevented from access to the underlying plaintext stored at S-CSP. In another word, the goal of the adversary is to retrieve and recover the files that do not belong to them. In our system, compared to the previous definition of data confidentiality based on convergent encryption, a higher level confidentiality is defined and achieved.

Results:

Screen Shots

Further Enhancement

Though the above solution supports the differential privilege duplicate, it is inherently subject to brute force attacks launched by the public cloud server, which can recover files falling into a known set. Will be insecure for predictable file. We design and implement a new system which could protect the security for predictable message. The *main idea* of our technique is that the novel encryption key generation algorithm. More specifically, Security is thus only possible when such a message is unpredictable. This traditional convergent encryption for simplicity, we will use the hash functions to define the tag generation functions and convergent keys in this section. In traditional convergent

encryption, to support duplicate check, the key is derived from the file *F* by using some cryptographic hash function.

Conclusion

In this paper, the notion of authorized data deduplication was proposed of users in the duplicate check. We also presented several to protect the data security by including differential privileges 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 schemes are secure in terms of insider and outsider server with private keys. Security analysis demonstrates that our attacks specified in the proposed security model of our proposed authorized duplicate check scheme and conduct testbed experiments on our prototype. As a proof of concept, we implemented a prototype we showed that our authorized duplicate check scheme incurs minimal overhead compared to convergent encryption and network transfer.

Acknowledgements

This work was supported by National Natural Science Foundation of China (NO.61100224 and NO.61272455),GRF CUHK 413813 from the Research Grant Council of Hong Kong, Distinguished Young Scholars Fund of Department of EducationCNS-1217889).

References:

[1] OpenSSL Project. http://www.openssl.org/.

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

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

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

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

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

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

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

[9] D. Ferraiolo and R. Kuhn. Role-based access controls. In *15th NIST-NCSC National Computer Security Conf.*, 1992.

[10]GNULibmicrohttpd.http://www.gnu.org/software/libmicrohttpd/.

[11] 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.

[12] 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.

[13] libcurl. http://curl.haxx.se/libcurl/.

[14] C. Ng and P. Lee. Revdedup: A reverse deduplication storagesystem optimized for reads to latest backups. In *Proc. of APSYS*,Apr 2013.

[15] W. K. Ng, Y. Wen, and H. Zhu. Private data deduplicationprotocols in cloud storage. In S. Ossowski and P. Lecca, editors,*Proceedings of the 27th Annual ACM Symposium on Applied Computing*,pages 441–446. ACM, 2012.

[16] R. D. Pietro and A. Sorniotti. Boosting efficiency and securityin proof of ownership for de duplication.In H. Y.Youm andY. Won, editors, *ACM Symposium on Information, Computer andCommunications Security*, pages 81–82. ACM, 2012.

[17] S. Quinlan and S. Dorward.Venti: a new approach to archivalstorage. In *Proc. USENIX FAST*, Jan 2002.

[18] 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 andversion control.In *3rd International Workshop on Security in CloudComputing*, 2011.

[19] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman.Role-based access control models. *IEEE Computer*, 29:38–47, Feb1996.

[20] J. Stanek, A. Sorniotti, E. Androulaki, and L. Kencl. A secure datadeduplication scheme for cloud storage. In*Technical Report*, 2013.

[21] M. W. Storer, K. Greenan, D. D. E. Long, and E. L. Miller. Securedata deduplication. In *Proc. of StorageSS*, 2008.