ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

PRIVILEGE RIGHTS BASED DATA PROTECTION SECURITY IN HYBRID CLOUD MODEL

K .Jagadeswari[1], Dr, P. Vivekanandan[2], Mr, G.bharathidhasan 3

M.E, Department of CSE, Park College of Engineering and Technology, Kaniyur.
H.O.D, Department of CSE, Park College of Engineering and Technology, Kaniyur.
Assistant Professor, Department of CSE, Park College of Engineering and Technology, Kaniyur.
Jagakrishna2101@gmail.com

Abstract:

Data deduplication is a data compression technique for eliminating duplicate copies of data and have been used in cloud storage to reduce amount of storage space. To protect the confidentiality of data, convergent encryption and symmetric encryption systems are used to encrypt the data prior to the outsourcing of data in cloud. To provide security for the data, shall be entitled to use data de-duplication scheme. In authorized duplication scheme user with privileges difference be considered in duplicate check. To support authorized duplicate check hybrid cloud architecture is introduced. Privilege key for each user is stored in the private cloud and data files stored in the public cloud with the help of S-CSP.

Key Words-Deduplication, authorized duplicate check, confidentiality, hybrid cloud.

1 INTRODUCTION

Cloud computing is an on-demand computing, where shared resources and information are available on request to computers and other devices. Cloud computing and storage solutions provide users and companies to store various functions and to process their data in third-party data centers. Cloud service providers offer both storage and computing resources at relatively low cost. Cloud computing will spread, amount of data stored in the cloud is an increased and shared by users with specified privileges that define the access rights of the stored data. A critical challenge in cloud storage services is the management of large amounts of data.

To manage the data stored in the cloud data deduplication technology has been used. Data deduplication is a data compression technique for eliminating duplicate copies of repetitive data in cloud storage. Deduplication identifies common data blocks into and between the files and stores them only once, deduplication can result in cost savings by increasing the usefulness of a given amount of memory. Deduplication is a technique that only one copy of each file on a storage server, regardless of how many customers are asking to save the file stores. Deduplication can take place either at the file level or block level. In the file-level deduplication duplicate copies of the same files are eliminated. In block-level deduplication duplicate copies of data blocks that will occur in non-identical files eliminated.

While the support of the deduplication, the data of the user vulnerable to both insiders and outsider's attacks. Provision of confidentiality to user data using conventional encryption scheme is incompatible with deduplication. In traditional encryption different users the file encrypted with its own key. So identical data will lead copies of different users in different ciphertexts, so that the duplication impossible. Convergent encryption [6] has been proposed to enforce the confidentiality of the data, while the deduplication possible. To encrypt a file with convergent encryption, first client calculates a cryptographically strong hash of the file contents. The file is then encrypted using this hash value as a key. The encryption process is deterministic and key derived from the data contents, identical copies of data are the same convergent key and thus to produce the same ciphertext.

To prevent unauthorized access, secure proof of ownership (POW) protocol [5], it is also necessary in order to prove that the user, in fact, has the same file, if a duplicate to be found. After proving, subsequent users will provided with pointer on the server available to the same file without upload the same file. A user can select the encrypted file with the pointer of the server that can only be decrypted by the corresponding data owners with their convergent key download. Thus, convergent encryption allows the cloud to perform deduplication on the ciphertexts and the proof of ownership prevents unauthorized users to access the file.

In authorized deduplication system, each user is uploaded to a number of privileges during system initialization .Each file to the cloud is limited by a number of privileges to specify what kind of users will be allowed to perform the duplicate check and access to the associated files. Before submitting a duplicate check request for a file, the user needs to take this file and its own privileges as inputs. The user is able to find a duplicate of this file if and only if it saved a copy of this file and a concerted privilege in cloud

1.1CONTRIBUTIONS

In this paper, an efficient deduplication to do with differential privileges in cloud computing, we consider the hybrid cloud architecture. It's a combination of both private and public cloud. Private cloud act as a proxy to allow data users to perform duplicate checking with differential privileges. The data owners store their data to public cloud with S-CSP, who lives on managed public cloud, in which all operations on data are performed by private cloud. The user may only perform the duplicate check for files with the appropriate privileges.

1.2 ORGANIZATION

In section 2 preliminaries of the paper is described. In section 3 system model for authorized deduplication system is proposed. A practical deduplication system with differential privileges in cloud computing are proposed in section 4

TABLE 1

Notations used in this paper

Acronym	Description
S-CSP	Storage Cloud Service Provider
PoW	Proof of Ownership
PU	Privilege set
skU	Users private key
pkU	Users public key

2 PRELIMINARIES

This section describes the terms used in this document and an overview of some basic elements of safe use in authorized deduplication. *Symmetric encryption.* A secret key algorithm is a cryptographic algorithm that uses the same key to encrypt and decrypt data. Common key k for encrypting and decrypting the files. KeyGenSE (1) -> k is the key generation algorithm which generates with security parameter 1 k; EncSE (k, M) -> C, the symmetric encryption algorithm, the secret k and the message M decreases, and then outputs the ciphertext C;DecSE (k, C) -> M is the symmetric decryption algorithm, which takes place the secret k and ciphertext C, and then the original message M.*Convergent Encryption.* The convergent key derived from the data copy and the data is encrypted with key converged. In addition to the main, also redirects users a day for the file where the tags are used to identify the duplicates. To recognize duplicates users calculates a tag and send to server side to check whether the identical copy has already been stored. Here we take on correctness property contains i.e if two copies of data equal then their tags are the same. The convergent and key tags can be derived regardless of the data copy. Copy of encrypted data and corresponding tag is stored in the client side.KeyGenCE (M) -> k is the key generation algorithm that a data card Copy M into a convergent key K.EncCE (k, M) -> C, the symmetric encryption algorithm, the copy is done, both the convergent key k and the M data as inputs and then outputs a ciphertext C.DecCE(k, C) -> M is the decryption algorithm which takes the cipher text C and the convergent key k as inputs and then to copy the original data M.TagGen (M) -> T (M) is the tag-generation algorithm which maps to copy the original data M and outputs a tag T (M).

Proof of Ownership. Proof of ownership allows the user to prove their ownership of copies of data to the storage server. It is implemented as an interactive algorithm is run by accountants and valuers. Accountants calculates hash value of the data copy. In order to prove their ownership of data copy y accountants send the hash value to the valuers. If the hash requested is not in the database of the server, users needs to upload the entire file. Otherwise, because the file to the server already exists, tells the client that there is no need to send the file itself. Both ways marked the server to the client as the owner of the file, and from that point on there is no difference between the client and the original participant who uploaded the file. The client can therefore ask you to restore the file, regardless of whether he was asked to upload the file or not. *Identification Protocol.* An identification protocol consist of two phases Proof and Check. In the detection, user U needs to prove its identity to a trial by conducting some proof of identification to prove his identity. The entry of the user's private key skU .The verifier shall conduct verification with the input of information to the public pkU together to article number. At the end of the audit, the auditors are available either accept or reject, to indicate whether the check is carried out or not.

3 SYSTEM MODEL

3.1 Hybrid Cloud Architecture for Secure Deduplication

There are 3 units define in our system, the user, private cloud, public cloud with S-CSP .The S-CSP is used to perform the deduplication, by checking whether the contents of the two files are the same, then it stores only a single file. Access to a particular file is defined with a set of permissions. For example, we define role-based access rights, or the time can be based privileges.In role-based authorization is an access control mechanism to define around roles where created the roles for various job functions. The permissions to perform certain operations are assigned to specific roles. Time-based access right specifies a valid period with the period file can beaccessed.

S-CSP. This is a unit that stores the user's data to cloud storage. To a scalable data management and reduce the cost of a memory S-CSP performs deduplication by eliminating copies of repetitive data. S-CSP stores only unique data.

User. This is an entity that, so it saves bandwidth and storage space by outsourcing their data to cloud with S-CSP .In deduplication system user uploads unique files. Each user file with convergent encryption to provide confidentiality of data encrypted.

Private Cloud. Private cloud is a semi-trusted third party, the privilege key for each user is stored. It act as an interface between users and public cloud. Before uploading the file to the cloud user needs to get a file token from the private cloud to perform deduplication.

3.2 Design Goals

This paper describes the privacy preserve deduplication and deduplication system should for support

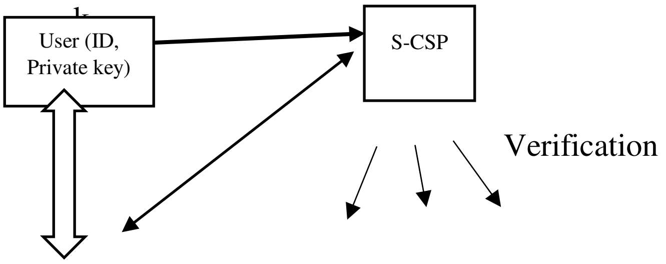
• Differential privilege authorization. To get ahead of the implementation of the duplicate check for a file needs of each user, a file token from the private cloud. Users can not token for duplicate check without appropriate privilege or without the help of the private cloud server.

• Authorized duplicate check. Authorized users need to prove their identity to private cloud for duplicate check token generation. After generating token user performs a duplicate check with public cloud using the duplicate check token of private cloud generated

This paper focuses on two types of securities, the security of the file token and the security of the data files. For the safety of the file token two aspects defined unforgeability and indistinguishability of the duplicate check token.

• Unforgeability of the duplicate check token. Authorized user receives only a duplicate check token from the private cloud. Unauthorized users cannot get without proper authorization token from the private cloud.

• Indistinguishable duplicate check token .Users cannot create a duplicate check token without private cloud and cannot create duplicate check token beyond their privilege.



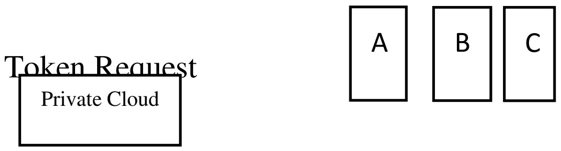


Figure 1 Architecture Diagram

4 AUTHORIZED DEDUPLICATION SYSTEM

To support authorized deduplication, file token is generated for the duplicate check to a file F and appropriate authorization. For each privilege p a secret key kp is limited. Φ'F, p = TagGen (F, kp) is a duplicate check token for file and F file can be accessed by users with authorization p. If a file with a duplicate check token Φ'F,p is uploaded then duplicate check for the file F is successful if and only if the user has file F and privileges p. The file tokens with cryptographic hash function H generates(.).

4.1SecureDeduplicationSystem

In safe deduplication, suppose there are N users in the system and a privilege universe as defined P = {p1, p2, ..., ps} .For every privilege p in P is associated with the private key kp. In authorized deduplication system hybrid cloud architecture is presented. The private key for the access rights are not published on the user directly stored and managed by private cloud server. In order needs to perform a duplicate check for a file user to obtain a file token from the private cloud server. To locate a file token user must obtain in order to send a request to the private cloud server.

The private cloud server checks the identity of any user and user to prove their identity with a secret key skU. After receiving the duplicate check token user can perform duplicates exam on public cloud servers. Based on the results of double checking the user either loads a file or running pow. Consider two privileges p and p ', p corresponding to p' if and only if R (p, p ') = 1 here, R is a binary relation.

System configuration. The privilege universe P = {p1, p2, ..., Ps} is defined. A private key kp for every privilege pi ∈P be selected, and a set of keys {kpi} pi∈P will be sent to the private cloud. Then, each user is assigned a secret key skU, and the keys are used to perform identification with servers. An identification protocol Π = (detection, check) defined .PoW protocol for file ownership is initialized. The private cloud server maintains a table that contains the privilege set PU and users public information and public key pkU.

Uploading files. Suppose the data owner wants to outsource a file F to public cloud and want to create a file with F user whose privilege is part of the authorization PF = {pj} .Before uploading the file user must want to perform a duplicate check. To perform a duplicate check users needs to obtain a file token from the private cloud. User proves their identity to private cloud using the secret key skU. If the proof is out the private cloud will recognize the user from the table permission. Initially, the user calculates File Tag & ΦF = TagGen (F) and send this tag to the private cloud servers. {Φ'F, pτ = TagGen (ΦF ,kpτ} returns back to the user and file token {Φ'F, pτ} send to S-CSP. When a duplicate file is found in a storage user needs to run Pow protocol to prove the ownership of file to the S-CSP. If the proof is passed user is provided with the pointer to the file .Then S-CSP provides a signature **σ** on the duplicate check token and time stamp on the receipt of the proof to the user. After that user sends the privilege set PF = {pj} along with returned proof by S-CSP to the user to the private cloud. Then private cloud checks proof of the S-

CSP returned. If the proof is passed then private cloud calculates $\{\Phi'F, p\tau = \mathrm{TagGen}\ (\Phi'F, kp\tau\}$ passed and sends it to the S-CSP together with the signature **σ**.Then the authorization of F association file PF and privileges set of data owners.

When a duplicate file is not present in the S-CSP then signature together with the authorization PF = {pj} is sent to private cloud. The private cloud server verifies the signature and then calculates $\{\Phi'F, p\tau = \mathrm{TagGen}\ (\Phi\ F, kp\tau\}$ send it to the S-CSP. The user then calculates a chipertext of CF = Enc (F file kF) where k is a convergent encryption key. Convergent key by calculating the hash value of the file kF = KeyGen (F) .After encrypt the file with the convergent Key-user-generated loads a CF with the S-CSP.

Retrieving file. When a user wants to download a file F, the user first sends a request and the file name to the S-CSP. After receiving the request from the user S-CSP checks whether the user is authorized to access the file F. If the user is authorized then chipertext CF of the file sent to the user , chipertext CF download is decrypt with the convergent key kF which are stored in the client machine .If user is not authorized to download then S-CSP sends a signal to the user to download show error

Problems. The authorized deduplication is started inherently subject to brute-force attacks by the public cloud servers. The brute-force attack can the files to recover under the well-known phrase. The destination file space of a ciphertext c can from a message space S = {F1, ..., Fn} of size n ,the public cloud servers F after at most n offline encryptions to recover. That is, i = 1, ..., N simple encrypted Fi to a ciphertext call to get through Ci. Convergent encryption provides security for files that are unpredictable it is unsafe for foreseeable files.

4.2 Proposed System Description

In the design of new encryption key generation algorithm, and hash functions used for tag generation. In Convergent encryption, the encryption key is deterministic, i.e keys are created with cryptographic hash function KF = H (F) .In this configuration encryption key is derived generated with private cloud server using authorization key kp. The F file is encrypted with the random key and k keys will be encrypted with kF, p. The encryption key can be as follows $kF, p = H0\ (H\ (F), kp) \oplus H2\ (F)$ .The private cloud server and S-CSP cannot be considered to decrypt the ciphertext. For S-CSP, if the file is unpredictable, it's certainly semantically secure. System configuration. The privilege universe P and the private key for each privilege, privilege universe maps. The Pow-defined protocol, and then also introduced identification protocol. Private cloud maintains a table where the table contains the permissions of each user and some public information about the user is stored.

Uploading files. If the data owner wants to create a file upload F and want the F file with users whose privilege belongs to the group P = {pj} .The data owners proves, their identity to the private cloud and then compute H (F) and send them to the private cloud. Then the private cloud calculates $\{\ \Phi F, p\tau = H0\ (H\ (F), kp\tau)\}$ .After receiving the ΦF, user sends it to the S-CSP for duplicate check. If the duplicate found then users run PoW to prove their ownership of datacopy, to the S-CSP. After the analysis is conducted, the user is provided with a pointer to the file. If the duplicate file is not then, together with the time stamp found signature, is sent to the user. Then, the user sends a signature and authorization {pj} to the private cloud. Private cloud checks the signature then calculates $\{\Phi F, pj = H0\ (H\ (F), kpj)\}$ and send it to the S-CSP and user. Then user calculates the encryption CF = Enc (k, F), where k is random key and the key is encrypted into the ciphertext {Ck, pj } with the key {kF,pj = ΦF, pj⊕H2 (F) .Finally the user uploads (CF, Ck, pj).

File Retrieving. During download { Ck,pj} is returned to the user. The user uses the key {kf,pj }to decode {Ck, pj } and obtains a key k. Then the user uses the k key to decrypt the original file F.

5 CONCLUSION

In this paper the notion of legitimate data deduplication has been proposed that data security by protecting differential privileges of users in the duplicate check. We presented some new deduplication support structures authorized duplicate check in hybrid cloud architecture, in which the double-checking tokens of files are generated by the private cloud server with private key. Convergent and symmetric encryption techniques used to protect the confidentiality of files.

REFERENCES

[1] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Dupless: Serveraided encryption for deduplicated storage," in Proc. 22nd USENIX Conf. Sec. Symp., 2013, pp. 179–194.

[2] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider, "Twin clouds: An architecture for secure cloud computing," in Proc.Workshop Cryptography Security Clouds, 2011, pp. 32–44.

[3] 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 Proc. Int. Conf. Distrib. Comput. Syst.,2002, pp. 617–624.

[4] D. Ferraiolo and R. Kuhn, "Role-based access controls, " in Proc.15th NIST-NCSC Nat. Comput. Security Conf., 1992, pp. 554–56

[5] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Proofs of ownership in remote storage systems," in Proc. ACM Conf. Comput.Commun. Security, 2011, pp. 491–500.

[6] J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," in Proc. IEEE Trans. Parallel Distrib. Syst., http:/doi.ieeecomputersociety.org/10.1109/TPDS.2013.284, 2013.

[7] W. K. Ng, Y. Wen, and H. Zhu, "Private data deduplication protocols in cloud storage," in Proc. 27th Annu. ACM Symp. Appl. Comput.,2012, pp. 441–446.

[8] R. D. Pietro and A. Sorniotti, "Boosting efficiency and security in proof of ownership for deduplication," in Proc. ACM Symp. Inf.,Comput. Commun. Security, 2012, pp. 81–82.

[9] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman,"Role-based access control models," IEEE Comput., vol. 29, no. 2,pp. 38–47, Feb. 1996.

[10] J. Xu, E.-C. Chang, and J. Zhou, "Weak leakage-resilient client side deduplication of encrypted data in cloud storage," in Proc.8th ACM SIGSAC Symp. Inform., Comput. Commun. Security, 2013,pp. 195–206.