Secure Data Sharing in Cloud Computing using Revocable Storage Identity-Based Encryption

S. Kalaivani[1]
Research Scholar,
Dept. of Computer Science,
Tamil University,
Thanjavur 613010,
Tamilnadu, India,
Email:kalaimphil17@gmail.com

A. Senthilkumar2
Asst. Professor,
Dept. of Computer Science,
Tamil University,
Thanjavur 613010,
Tamilnadu, India,
Erodesenthilkumar@gmail.com

Abstract: Nowadays regularly use cloud services in our daily life.There are various services provided by cloud such as a service, Platform as a service, and Infrastructure asa service. The used to keep our data,documents, and files on cloud. The data that store may be Personal, Private, secret data. So must be very sure that whatever the cloud service we use that must be secure. Cloud computing Provides number of services to client over internet. Storage service isone ofthe important services that people used now days for storing data on network so that they can access their data from anywhere and anytime. With the benefit of storage service there is an issue of security. To overcome security problem the proposed system contain two levels of security and to reduce the unwanted storage space de-duplication[1,2] technique is involved.

To increase the level of security one technique is a session password.Session passwords can be used only once and every time a new password is generated.To protect the confidentiality of sensitive data while supporting de-duplication[1,2]the convergent encryption technique has been proposed to encrypt the data before outsourcing,Symmetrickey algorithm uses same key for both encryption and decryption.In this paper,I will focus on session based authentication for both encryptions for files and duplication check for reduce space of storage on cloud.

***Keywords**:cloud Computing, security, privacy, Secret data, Deduplication.*

*****

I. INTRODUCTION

Cloud offers various services to the user. Data storage service provided by cloud is the most commonly used service given by cloud.User used to upload data onto the cloud and let cloud to manage that data.Data may be in the files which can be personal or private.As user is storing data onto the cloud,user has to pay rent for storing data.Data storage rent may very different cloud service provider but as user is paying rent and if user is storing the same copy of data on cloud multiple times then the rent will store the data on cloud only once same copy of data onto cloud then user must be requiring security to data.For the security purpose datais get stored on the cloud in the encrypted format.So Deduplication checking has to be performed on the encrypted data. User will store the data on the cloud in encrypted format and then it is checked that whether that data is already present on the cloud or not.If the data that user want to storeonto the cloud is already present then duplication occur.User will also store data in encrypted format duplication check will also be performed on the data present on the cloud which is also store data in encrypted data. It is complicated for the data holder to check the Deduplication on encrypted data.In this scheme the data ownership challenge and proxy re-encryption is used to manage encrypted data storage with Deduplication.

With the unremitting and exponential increase of the number of users and size of their data, data Deduplication becomes more and more a requirement for cloud storage providers.By storing aexclusive copy of duplicate data,cloud breadwinnersgreatly reduce theirstoring and data transfer costs.These huge volumes of data need some practical boards for the storage,processing and availability and cloud technology offers all the possibilities to fulfill these requirements.Data Deduplication [1,2] is referred to as a approach offered to cloud storage providers (CSPs)to eradicatethe duplicate data and keep only a single exclusivecopy if it for storing space saving determination.

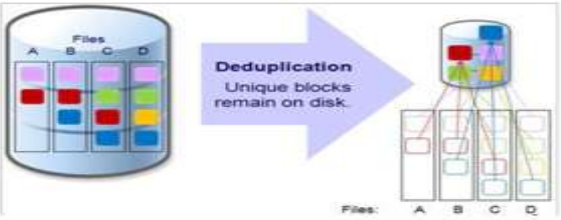

Fig.1. Data-Deduplication

By guardianship a single copy of repeated data,statisticsDeduplication is considered as one of the most promising solutions to diminish the storage,costs, and improve user'sknowledge by saving network bandwidth and reducing backup time.The compensations of Deduplication[1, 2] unfortunately come with a high cost in terms of new security and privacy encounters. Deduplication can take place at either the file level or the block level. For file level Deduplication,it removes duplicate reproductions of the same file.Deduplication can also take place at the chunk level,whichremoves duplicate blocks of data that occur in non-identical documentations.

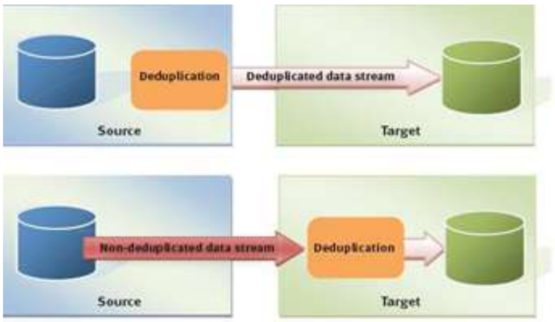

Fig.2. Deduplication at source and at target location

Depending on the participating machines and steps in the customized deduplication process,it is either performed on the client machine(source -side) or near the final Storage-server(target-side).It the former case ,duplicates are removed before the data is transmitted to its storage.Since that conserves network bandwidth,this option is particularly useful for clients with limited upload bandwidth.

Convergent encryption[3,4,5]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 cryptography hash value of the data copy.After key generation and data encryption,users retain the keys and send the cipher text to the cloud.Since the encryption operation is deterministic and is derived from the data content,identical data copies will generate same convergent key and hence the same cipher text.To prevent unauthorized access,a secure proof of ownership protocol[6,7] is also needed to provide the proof that the user indeed owns the same file will file when duplicate is found.After the proof,subsequent users with the same file will the same file will be Depending on the participating machines and steps in the customized Deduplication process, it is either performed on the client machine(source-side) or near the final Storage-server(target-side).

In the former case,duplicates are removed before the data is transmitted to its storage.Since that preserves network bandwidth,this option is predominantlyvaluable for clients with incomplete upload bandwidth.

Convergent encryption[3, 4, 5] has been proposed toadminister data confidentiality while manufactureDeduplicationpossible.Itencrypts/decrypts a data copy with a convergent keywhich is obtained by computing the cryptographic hash value of value of the gratified of the data copy, after key regiment and data encryption, users retain the keys and send and the cipher text to the cloud.Since the encryption operation is deterministic and is derived from the data content identical data copies will generate same convergent key and hence the same cipher text.To prevent unauthorized access,a secure proof of ownership protocol[6,7]is also needed to provide the proof that the user indeed owns the same file when a duplicate is found.After the proof, subsequent users with the same file

II. SYSTEM ANALYSIS:

EXISTING SYSTEM

For these problems,in this paper there is ABE,Attribute based encryption,Scheme is used.To ensure data privacy, existing research proposes to outsources only encryption data to CSPs.Existing solutions for deduplication are vulnerable to brute-force attacks and can't flexibly support data aces control and revocation.

Different fromoutmoded de duplication systems, in the existing system the dissimilar privileges of users are considered in duplicate check besides the data itself. To support sanctionedrepetition, the tag of a file will be strong-minded by the file and the privilege. To show the difference with traditional representation of tag, we call it file token in its place. To support authorized access, a secret key will be bounded with a privilege p to generate a file token

DISADVANTAGES:

(1) They cannot flexibly support data access control and revocation

(2) The result of encryption is to make encryption data copy which cannot be distinguishable after being encrypted.

(3) The main disadvantage of this algorithm is early execution of the large task might increase the total response time of the system

PROPOSED SYSTEM:

Proposed prototype is secured in terms of upload and downloads data operation on hybrid cloud,and also achieving 100% deduplication ratio for cloud storage. Convergent encryption technique is proposed to enforce confidentiality during de-duplication,which encrypts data before outsourcing.A unique modification to the Improved Max-min algorithm is proposed .Proposed on Improved where instead of selecting the largest task. Proposed a system in which they are using block level deduplication duplicate check is proposed.proposed a system,in which to reduce the workload due to duplicate file,proposed the index name server(INS)to manage not only file storage,data de-duplication ,optimized node selection, and sever load balancing, but also file compression, chunk matching ,real-time feedback control, IP information ,and level index monitoring

ADVANTAGE:

(1)The main object of this work is to study and compare a variety of task scheduling algorithms are used in the cloud computing.

(2) The advantage of Deduplication unfortunately comes with a high cost in terms of new security and privacy challenges.

(3)De-duplication technique is used to check whether the uploaded document is already existing on cloud server or not

III. NUMBER OF MODULES:

After careful analysis the system has been identified to have the following modules

1. Key owner
2. CloudKey Bank provider
3. Trusted client
4. User

MODULE Description:

❖ Key owner:

Key owner can be the password owner or data encryption key who outsources his/her encrypted key database (key DB) to the cloud Key Bank provider.After that the converted key databasestored in cloud Key-Bank provider can be retrieved anywhere and anytime with minimum evidence leakage such as the size of Key DB.The key owner mostly completes the subsequent three tasks: 1)Building the customized access control policy(ACP) In terms of his/her applied keys sharing requirements;2) Depositing key DB by using deposit key procedure under the support of ACP;3) Dispensing authorized Query tokens to the vicarious user based on the user's enumeratedmaterial such as the wanted query and corporeal and identity.

❖ Cloud Key Bank provider:

Cloud Key bank provider can be any professional password manager such as last pass who provides privacy enforced access control on EDB. The cloud KeyBank provider mainly finishes the following two tasks: 1) To implement the privacy of identity characteristics in the search attribute group, he/she can accomplish search query straight by evaluating the submitted Query token against the encrypted Key tuples in EDB; 2) To implement the Key authorization he/she can transform an encrypted Key into the sanctioned re-encrypted Key under the consistentEntrustment token stored in AuthorizationTable (AUT).

❖ Trusted client:

Trusted client is the primary privacy enforced component in cloud Key Bank framework It mainly consists of two protocols;Deposit Key and Withdraw Key. Deposit Key protocol provides Key DB encryption,symbolic generation(including Query token and Entrustment token).Withdraw Key proceduredelivers the re-encryption Keys of encryption keys and the decryption of re-encryption Keys.

❖ User:

There are two varieties of users in cloud Key Bankbackground: Key owner and collaboration group. Key owner resemblesto aseparate user who deposits all his Keys to cloud Key Bank provider and accesses them by himself. Partnership to a group of users where the Key owner can share his/her Keys with other users within the same teamwork group.By submitting the private Key and authorized Query token, a delegated user can remove an authorized Key by using Withdraw Key procedure under the provision of privacy compulsory access control policy (i.e. AUT in our answer).

IV. CONCLUSION:

To solve the recognized critical security supplies for Keys outsourcing .We present cloud Key Bank, the first unified privacy and owner agreement enforced Key management framework. To implement cloud KeyBank, suggest a new Cryptographic embryonic SC-PRE and the consistent concrete SC-PRE arrangement. The security contrast and analysis prove that our solution is adequate to support the identified three security requirements which are not be solve in old-style outsourced scenario. From the performance analysis, can see that our explanation is not so efficient because it necessitates several seconds to answer a query on a database only 200 keywords.

V. FUTURE ENHANCEMENT:

Regionalized Access Control In this paper, around is one cryptosystem in each data submission and the data owner acts as the only consultant in each cryptosystem. Operation on Encrypted Data When encryption provides data confidentiality, it also greatly limits the flexibility of data operation .Another interesting future work would be taking into account information theoretic techniques from the areas such as database privacy .In order for doing so, one interesting future work would be integrating techniques from trusted computing into the data access control mechanism.

REFERRENCES:

[1] S. Bugiel, S. N¨ urn Berger, A. Sadeghi, and T. Schneider, “Twin clouds: Secure cloud computing with low latency - (full version),”in Communications and Multimedia Security, 12th IFIP TC 6 / TC11 International Conference, CMS 2011, Ghent, Belgium, October 19-21,2011.

Proceedings, ser. Lecture Notes in Computer Science, vol.7025. Springer, 2011, pp. 32–44.

[2] M. Fischlin and R. Fischlin, "Efficient non-malleable commitmentschemes," in Advances in Cryptology - CRYPTO 2000, 20th AnnualInternational Cryptology Conference, Santa Barbara, California, USA,August 20-24, 2000, Proceedings, ser. Lecture Notes in ComputerScience, vol. 1880. Springer, 2000, pp. 413–431.

[3] D. Quick, B. Martini, and K. R. Choo, Cloud StorageForensics. Syngress Publishing / Elsevier, 2014. [Online].Available: http://www.elsevier.com/books/cloud-storageforensics/quick/978-0-12-419970-5

[4] B. Zhu, K. Li, and R. H. Patterson, "Avoiding the disk bottleneckin the data domain deduplication file system," in 6th USENIXConference on File and Storage Technologies, FAST 2008, February 26-29, 2008, San Jose, CA, USA. USENIX, 2008, pp. 269–282.

[5] M.Bellare and S. Keelveedhi, "Interactive message-locked encryptionand secure deduplication," in Public-Key Cryptography – PKC2015 - 18th IACR International Conference on Practice and Theory inPublic-Key Cryptography, Gaithersburg, MD, USA, March 30 – April1, 2015, Proceedings, ser. Lecture Notes in Computer Science, vol.9020. Springer, 2015, pp. 516–538.

[6] K. R. Choo, M. Herman, M. Iorga, and B. Martini, "Cloud forensics:State-of-the-art and future directions," Digital Investigation,vol. 18, pp. 77–78, 2016.

[7] D. Quick and K. R. Choo, "Google drive: Forensic analysis of data remnants," J. Network and Computer Applications, vol. 40, pp. 179–193, 2014.