International Journal of Scientific Research in Engineering and Management(IJSREM)
Volume: 03 Issue: 06 | June -2019 ISSN: 2590-1892

ENCODED INFORMATION STORAGE IN CLOUD WITH SECURE DEDUPLICATION BASED ON TRAIT

PAVITHRA.N
PG Scholar, Dept of MCA
Dayananda Sagar College of Engineering
Bangalore, India

Prof. RAKSHITHA KIRAN P
Dept of Master of Computer Applications
Dayananda Sagar College of Engineering
Bangalore, India

Abstract - Cloud computing encourages data providers who need to redistribute their information to the cloud without uncovering their sensitive information to external users and might want clients with specific credentials to have the option to get to the information . This expects information to be put away in encoded shapes with access control approaches to such an extent that nobody aside from clients with attributes of explicit forms can decrypt the encrypted information. An encryption strategy that meets this necessity is called trait based encryption, where a client's private key is related with a property set, a message is encrypted under an access policy over a lot of properties, and a client can decrypt a ciphertext with his/her private key if his/her arrangement of characteristics fulfills the access policy approach related with this ciphertext.

Trait based encryption has been broadly utilized in distributed computing where an information provider redistributes his/her encrypted information to a cloud service provider, and can impart the information to clients having explicit certifications.So,in this paper we suggest a way to encrypt the data and with secure deduplication and store the data into the cloud.

Keywords- cloud computing ,deduplication , access control, key generation.

1. INTRODUCTION

Cloud computing plans introduced warehoused information, where the re-appropriated information is kept unaltered over remote servers .In cloud information stockpiling framework, clients are able to store their information in the cloud and no longer have the information locally .

A method which has been embraced to oversee huge excess information is Deduplication which assumes a key job in Cloud Computing administrations. The essential idea behind deduplication is to store duplicate data just once.

Likewise, if a customer needs to move a record which is presently secured, the cloud provider will add the customer to the owner summary of that report. Deduplication has shown to achieve high space and cost hold reserves and various huge information storing providers are starting to accept it.

2. METHODOLOGIES

SYSTEM DESIGN

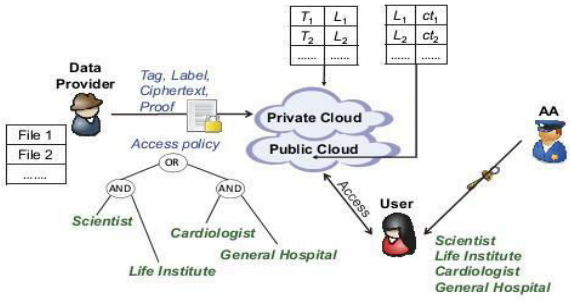

Fig.1.Process of deduplication of encrypted data

The above diagram shows the storage of data in cloud with secure deduplication .The data owner is responsible for uploading the information to the cloud storage system. Before being transferred to the cloud the information experiences the cipher content procedure where information is encoded. The information goes to the private cloud to check for the deduplication procedure where tag, mark and figure content are utilized. The benefit of this procedure is thatinformation is encoded before it is transferred into the cloud.

The public cloud is reponsible for managing the deduplicated files and storing the files. For accessing the public cloud by user ,attribute based access policy is used .Access policy works in away where the user has access to the cloud or not and if the user has no access, he cannot download or access the data from the cloud.

VIEW THROUGHPUT RESULTS

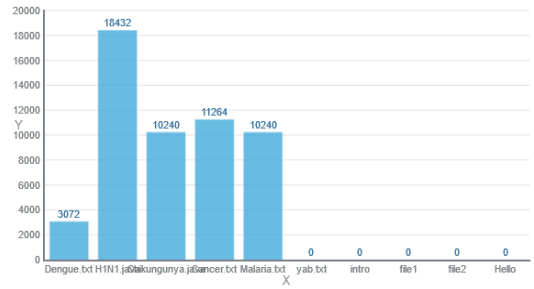

Fig.2.Throughput results

VIEW TIME DELAY RESULTS

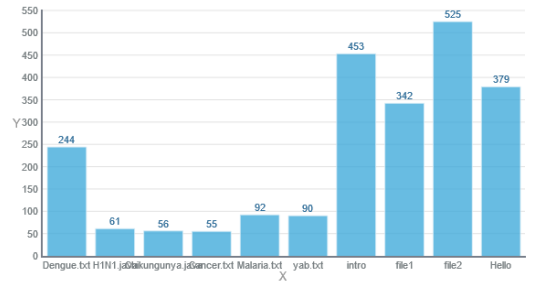

Fig.3.Time delay results

3. EXISTING SYSTEM

When a user uploads data which is already present within the cloud storage system , the user ought to be deterred from accessing the information that were hold on before he obtained the ownership by uploading it . These dynamic ownership changes might occur terriblyoftin a verypractical cloud system, and thus, it ought to be properly managed so as to avoid the safety degradation of the cloud service. The expert needs to give consent for the record or information to be transferred by the data owner. The information can be seen or sought or downloaded by the individuals who gets the consent or permission from the data owner. On the off chance that two clients transfer a similar document, the cloud server can recognize the equivalent ciphertexts and store just a single duplicate of them.

4. PROPOSED SYSTEM

In this paper, we present a trait based capacity structure which uses ciphertext-course of action characteristic based encryption and supports secure deduplication. Initially, the framework is the principle that achieves the standard thought of semantic security for data secrecy in trait based deduplication systems by going to the hybrid cloud engineering.

Besides, we put forward a method to alter a ciphertext more than one access methodology into ciphertexts of the comparable plaintext anyway under some different access approaches without revealing the fundamental plaintext.This strategy might be of independent excitement for development to the application in the proposed stockpiling framework.

5. DESIGN

USER REGISTRATION AND CLOUD ACCESS

User has to first register to the cloud . After the cloud authorize the user, then user will have the permission to download or search the file .Before the registration of cloud services to see whether the client is

authenticated or not to access cloud server,can ensure whether the information stored in the cloud is used judiciously by the responsible stakeholders as per the service level agreements.

UPLOADING THE FILE

The data owner or user has to upload the file

to the cloud.First, the user has to be authorized by the cloud with decryption key and then the file has to be uploaded to the cloud.

TRAIT BASED STORAGE SYSTEM

Our storage system is built with the use of hybrid cloud architecture, where a private cloud manipulates the computation and a public cloud is responsible for managing the storage. Trait based encoded information storage to cloud with secure deduplication, in which the cloud doesn't store the file multiple times despite the fact that it might get numerous duplicates of a similar record scrambled under various access strategies.

6. CONCLUSION

Trait based encryption has been generally used in cloud computing where data providers or data owners redistribute their encoded information to the cloud storage server and can share the encoded information to clients having specified credentials. Then again, de-duplication is a significant method to spare the storage space and network bandwidth capacity, which disposes duplicate copies of identical information.

The proposed storage system appreciates two advantages; it tends to privately share information to different viewers by indicating an access policy rather than sharing the decryption key. Besides, it accomplishes the security.

Therefore, reliable and efficient key generation system will be helpul for deduplication. Furthermore data increasing will result in the increase of the cloud storage.

7. FUTURE ENHANCEMENT

Future work includes effective checking of the ownership information, and information access constrained by either the information owner or its delegate specialist.Providing flexible data update and sharing with de-duplication even when the data holders are offline or online and also make it to achieve more accuracy, efficient and reliable .Presently,we are encrypting and decrypting the files which are in text format and not audio,video and images and this can be done for future work.

REFERENCES

1) J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou. Secure deduplication with efficient and reliable convergent key management. In IEEE Transactions on Parallel and Distributed Systems, 2013.

2) Attribute Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud, Hui Cui, Robert H. Deng, Yingjiu Li, guowei, IEEE Transactions on Bog Data, 2017.

3) W. K. Ng, Y. Wen, and H. Zhu. Private data deduplication protocols 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.