ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

Storage Security and Dynamic Deduplication of Data in Cloud

Shubhashini K L [1], Prasanna Kumar M [2]

P.G. Student, Department of Computer Science & Engineering, East West Institute of Technology, Bangalore, Karnataka, India[1]

Associate Professor, Department of Computer Science & Engineering, East West Institute of Technology, Bangalore, Karnataka, India[2]

ABSTRACT: Data deduplication is one of the effective methods for compressing data in a cloud environment which involves eliminating duplicate copies of repeating data, and has been widely used in cloud storage to reduce the amount of storage space and save bandwidth in cloud environment. To ensure proof of storage for sensitive data while supporting deduplication, the AES encryption technique has been proposed to encrypt the data before outsourcing.

KEYWORDS: Data Encryption, Cloud Storage, Deduplication of Data.

I. INTRODUCTION

The cloud service providers will give a number of computing resources and storage space for plenty of users at a very reasonable cost. Because of increasing number of cloud users, an increasing amount of data is being stored in the cloud with certain access privileges. The main problem of cloud storage services is the management of ever-increasing volume of data. To eliminate the redundancy of data in cloud computing, deduplication is the best technique and has attracted more and more attention recently. Data deduplication is a specialized data compression method which involves eliminating duplicate copies of repeating data in storage. The method is used to improve space utilization instead of keeping multiple data copies with the same content, deduplication eliminates redundant data by keeping only one physical copy and referring other redundant data to that copy. Deduplication can be applied either to file level or the block level. In case of file level deduplication, it eliminates duplicate copies of the same file. Whereas in case of block level deduplication, it eliminates duplicate blocks of data that occur in non-identical files.

II. LITERATURE SURVEY

1. 2016-A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data.
Author : Z. Xia, X. Wang, X. Sun, and Q. Wang

Due to the increasing usage of cloud services because of its flexibity to data access and storage, cloud computing has become popular, many users and data owners are influenced and motivated to outsource their data to cloud servers for great ease and reduced cost in data management. However, the confedential data should be encrypted before outsourcing the data for privacy requirements, which outdate data usage like keyword based document retrieval.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

In this paper, the encrypted cloud data will be searched using a safe multi keyword ranked search scheme, which supports dynamic update operations like deletion and insertion of documents. "Greedy Depth first Search" algorithm is used to provide accurate multi keyword ranked search.

The kNN algorithm is used to encrypt the index and ensure exact relevance score calculation between encrypted index and query vectors.

2. 2015-From Security to Assurance in the Cloud: A Survey.

Author : C. A. Ardagna, R. Asal, E. Damiani, and Q. H. Vu.

The cloud computing today has become an important platform for the distribution of business processes and applications. In Current ERA, many softwares, frameworks are working on a "Pay and Use" model. Cloud users are offered valuable cloud resources at low prices, and high performance and flexibility, than other service providers. Still, cloud users are worried with the cloud's level of service and the fancy properties on latest trends. The research association is concentrating more on the fancy aspects of the cloud paradigm, among which cloud security stands out. The survey in this article concentrates primarily on cloud security and cloud security assurance. First, we start with an analysis on art of cloud. Second, we introduce the approach of cloud security assurance and analyze its growing brunt on cloud security approaches. Finally, we present some prototypes for the development of next generation cloud security and assurance solutions.

3. 2013-Security and privacy in cloud computing.

Author : Z. Xiao and Y. Xiao

Recent updates have given increase in popularity and success of cloud computing. However, when outsourcing the data and business application to a third party increases the security and privacy issues to become a critical threat. The most important attributes to be considered for security and privacy are confidentiality, integrity, availability, accountability, and privacy preservability. Starting with these attributes, we analyse the relationships among them, the faults, the loop holes that can be identified by hackers, the weakness that may be exploited by attackers, the threat models, as well as existing defense strategies in a cloud environment. Further research directions are previously determined for each attribute.

III. SYSTEM MODEL

User Module:

All the authenticated users will be having access to the cloud system. Every user should have an account or they should first register to get access to the system.

Secured DeDuplication System:

To support authorized access, a secret key K will be generated for every file F and the file can be accessed only when that secret key is provided. As a result, if a file has been uploaded by a user with a duplicate key then a duplicate check sent from another user will be successful if and only if he also has the file *F* and access privilege. Such a key generation function could be easily implemented as $H(F, K)$, where $H(\_)$ denotes a cryptographic hash function.

An authorised user can login using Username and Password. Upon sending a file to cloud server, a secret key for the encrypted block of file will be generated and it will be shared to Admin. The sender himself has to provide the secret key in order to download that block of file.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

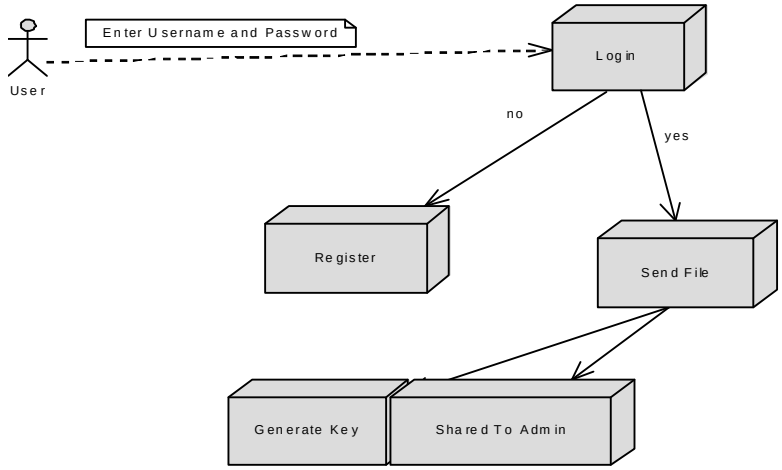

Fig. 1. Component diagram for sender

An authorised user can login using Username and Password. To download a file from cloud server, the secret key should be provided. The Receiver should first send a request for secret key to the sender. The sender can either accept or reject the request.

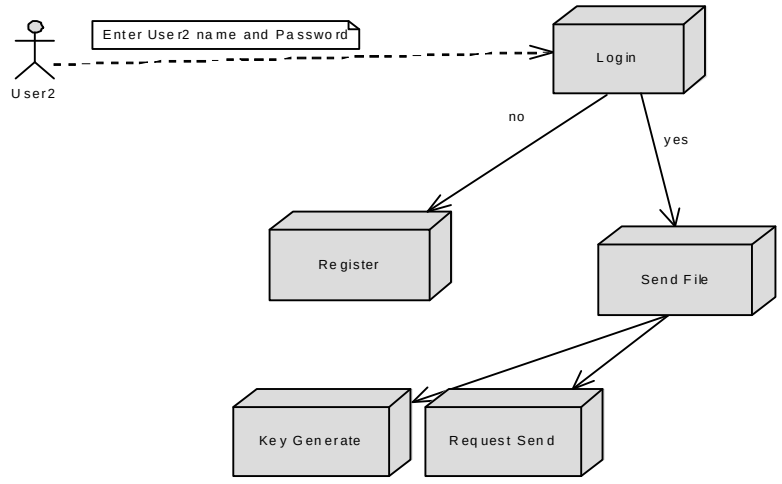

Fig. 2. Component diagram for Receiver

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

Send Key:

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

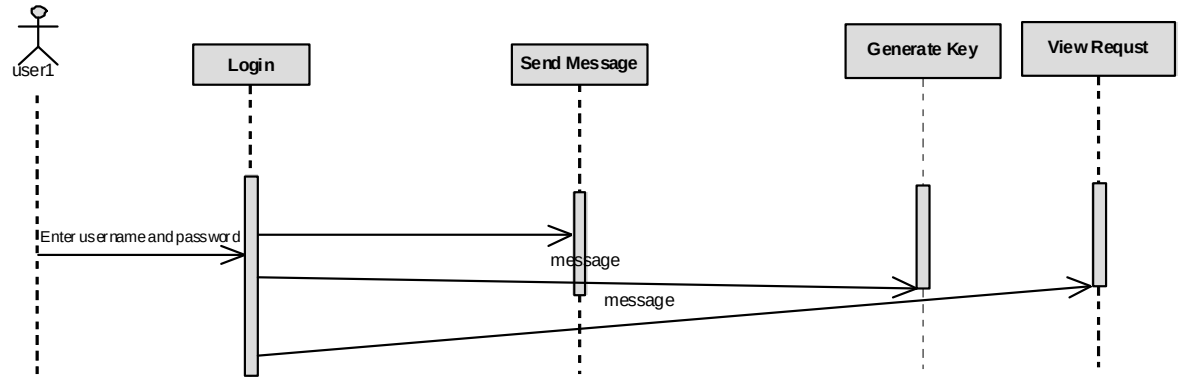

Fig. 3. The Sequence Diagram for Sender User

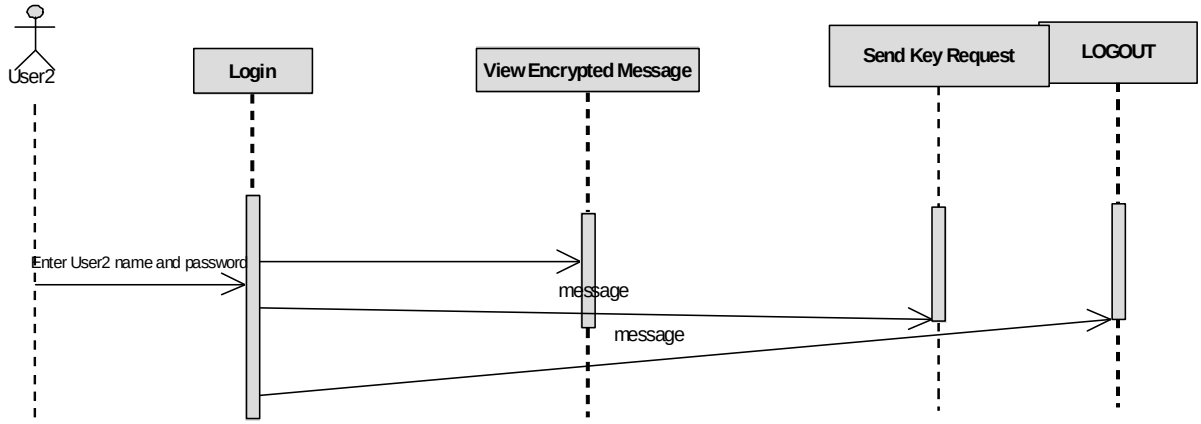

Fig. 4. The Sequence Diagram for Receiver User

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

IV. EXISTING SYSTEM

The cloud service providers will give a number of computing resources and storage space for plenty of users at a very reasonable cost. Because of increasing number of cloud users, an increasing amount of data is being stored in the cloud with certain access privileges. Even though there is a security for the data, the storage is not used in an efficient manner.

DISADVANTAGES:
The main problem of existing system 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 outsourcing. To ensure that the outsourced data is secured, this paper first addressed the issue of data deduplication. This technique is different from the traditional deduplication schemes since the differential privileges of users are further considered in duplicate check besides the data itself. We have used efficient deduplication constructions to eliminate the duplicate copies of data being saved in cloud environment. As a proof of storage, we encrypt the data in the file by using Advanced Encryption Standard algorithm before storing the data in cloud.

ADVANTAGES:
One critical challenge of cloud storage services is the management of the ever-increasing volume of data. Data Deduplication scheme overcomes this problem.

VI. CONCLUSION

Here we used data encryption method in an efficient manner to ensure high data security in cloud. Existing system did not address the problem of efficient space management in cloud environment for that we proposed data deduplication concept for eliminating duplicate copies of repeating data.

REFERENCES

[1] Kun He, Jing Chen, Ruiying Du, Qianhong Wu, Guoliang Xue, and Xiang Zhang "DeyPoS: Deduplicatable Dynamic Proof of Storage for Multi-User Environments ",IEEE Transactions on Computers, 2016
[2] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 2, pp. 340–352, 2016.
[3] C. A. Ardagna, R. Asal, E. Damiani, and Q. H. Vu, "From Security to Assurance in the Cloud: A Survey," *ACM Comput. Surv.*, vol. 48, no. 1, pp. 2:1–2:50, 2015.
[4] F. Armknecht, J.-M. Bohli, G. O. Karame, Z. Liu, and C. A. Reuter, "Outsourced proofs of retrievability," in *Proc. of CCS*, pp. 831–843, 2014.
[5] R. Du, L. Deng, J. Chen, K. He, and M. Zheng, "Proofs of ownership and retrievability in cloud storage," in *Proc. of TrustCom*, 328–335, 2014
[6] J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou, "Secure Dedupli cation with Efficient and Reliable Convergent Key Management," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 6, pp. 1615–1625, 2014.
[7] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Communications Surveys Tutorials*, vol. 15, no. 2, pp. 843–859, 2013.
[8] Q. Zheng and S. Xu, "Secure and efficient proof of storage with deduplication," in *Proc. of CODASPY*, pp. 1–12, 2012.
[9] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *Proc. of INFOCOM*, pp. 1–9, 2010.