International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 2, Issue 6, June 2015, PP 16-18
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

An Efficient Secure Authorized Data Deduplication Approach in Cloud Computing

M.Parabrahma Rao[1], Gunthati Prathap[2]

[1] Dept. of Computer Science and Engineering, SVIST Kadapa, A.P, INDIA
[2] Dept. of Computer Science and Engineering, SVIST Kadapa, A.P, INDIA

Abstract: *Nowadays very difficult to store the data in secure manner. Most of the internet users suffer from security problems. To store the data in the cloud is easy task but the major issue here security .In cloud lot of is redundant data present so most of the space filled with replicated information it also a major challenge. Previous papers are described about deduplication with low security algorithms. Example symmetric algorithms are used to provide security. IN this paper we proposed high security public-key algorithms and for authentication purpose we extend various algorithms. Finally we protect the cloud from unauthorized access and also eliminate the replicated data using deduplication technique.*

Keywords: *cloud computing, public-key cryptography, deduplication, Kerberos.*

1. Introduction

Cloud computing is global virtual resource it provide service to users across the internet. For past few years back data will stored in hard disk and some other external storage devices. But very difficult to carry the data to along the users. So in recent year's user data store in huge virtual storage location that is cloud.The cloud is large storage area to internet users here to upload and retrieve the data easily. It's called cloud computing. Some users are stored same kind of information with different file names so due to the reason replication problem could arise. Lot of space filled with duplicated data. it is major problem for the cloud computing. Here using deduplication compression techniques are used to control and elimate the redundant data. Example if file will already save with some X file name suppose fortunately or unfortunately copy the same file gain in different location replication problem arise but using deduplication compression technique eliminate the duplicate file. But same file will be copied again if the file having any updating happens rather than the existed files. In cloud computing uploading data or files are easy task, but protect the data in secure is serious problem. IN the Existing paper using symmetric algorithm for authentication and retrieve the file from the cloud.

Symmetric Algorithm: Basically it is better algorithm to encrypt the data at huge, same key using both encryption and decryption process. By using symmetric key the attacker easy to break the keys because if the attacker find any of the encryption key, the same key using at the time of decryption. in this algorithm very useful for encrypt use amount of data.

Public-key Algorithm: It provide most security than symmentric.using different keys for both encryption and decryption process. Those are public and private keys.

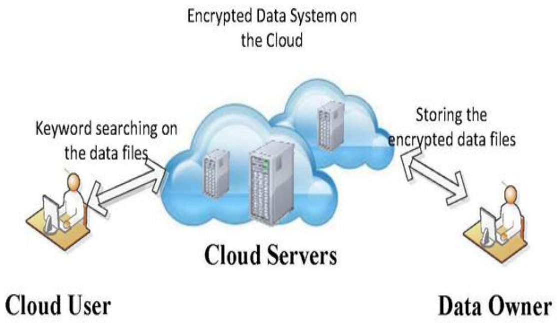
Private keys only known by users, public keys are universal keys. For authentication purpose using private key for encryption by the user public key for the decryption by the destination user. For confidentiality using public key for encryption by the user and private for decryption at end user.

In this Paper we proposed using efficient authentication **Kerberos Algorithm**.

2. Existing System

In Existing system User freely to upload the load frequently. To eliminate the redundant information on cloud used deduplication compression method. The upload the files in encrypted manner. Those who are known the key having the access permissions.

The cloud filled with encrypted data files.


Encrypted Data System on the Cloud
Keyword searching on the data files
Storing the encrypted data files
Cloud Servers
Cloud User
Data Owner

From the fig.Data owner upload the files to cloud by applying various symmetric algorithms.

Cloud allows any kind of information from the data owners. But in case of cloud user searching any kind of files from the cloud, if find any of the file before download it the cloud user know the corresponding decryption keys. If it matches then retrieve the file.in existing system use symmetric keys for data security. There is no proper Authentication scheme to avoid unauthorized users.

3. Proposed System

The proposed system enhancing the properties of existing systems.

The following steps are:

a) Encryption

b) Authentication

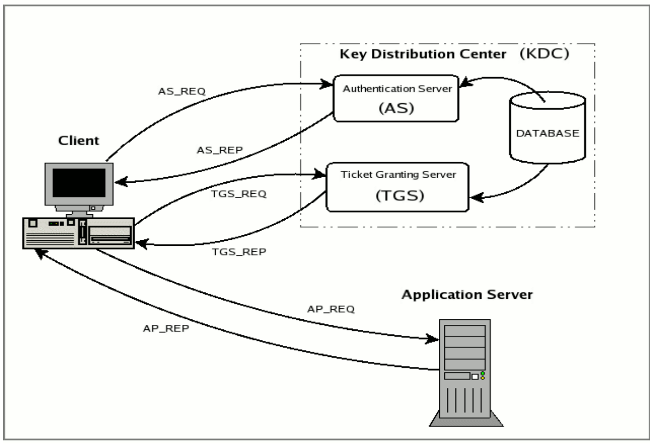
c) Confidentiality

a) Encryption:

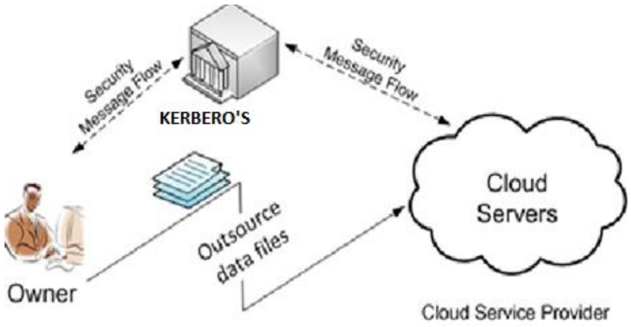
Encryption process using public key algorithms. Using different keys for both encryption and decryption process in increase security levels.

b) Authentication

In Authentication phase using classical Kerberos's algorithm to protect from unauthorized access. From the fig shows KDC provide interface to the server. KDC has AS, TGS and DB.it generate session valid interface from client to server. But it valid only during the session time only.


Key Distribution Center (KDC)
Authentication Server (AS)
DATABASE
Ticket Granting Server (TGS)
Client
AS_REQ
AS_REP
TGS_REQ
TGS_REP
Application Server
AP_REQ
AP_REP

c) Confidentiality



The client send the data in secure manner through the session interface before it could expire.to continue the same connection no need to contact KDC again, choose same connection until to complete the task. For secure files upload/downloads using Kerberos for outsource files transmit in normal way.

4. Conclusion

The most of the main issues with cloud computing have been addressed to a degree that clouds have become interesting for full commercial exploitation. This however does not mean that all the problems listed above have actually been solved. Cloud computing is therefore still as much a research topic, as it is a market offering. For better authentication confidentiality and security in cloud computing we have proposed new deduplication constructions using secure algorithms it supporting for authorized duplicate check in efficient cloud architecture, in which the duplicate-check tokens of files are generated by the with symmetric keys. Proposed system includes proof of data owner (Authentication) so it will help to implement better security issues in cloud computing**.**

References

[1]. Meister, D., Brinkmann, A.: Multi-level comparison of data deduplication in a backup scenario. In: SYSTOR ’09, New York, NY, USA, ACM (2009) 8:1–8:12

[2]. Douceur, J.R., Adya, A., Bolosky, W.J., Simon, D., Theimer, M.: Reclaiming space from duplicate files in a serverless distributed file system. In: ICDCS ’02, Washington, DC, USA, IEEE Computer Society (2002) 617–632

[3]. Harnik, D., Pinkas, B., Shulman-Peleg, A.: Side channels in cloud services: Deduplication in cloud storage. Security Privacy, IEEE 8(6) (nov.-dec. 2010) 40 –47

[4]. 4.K. Zhang, X. Zhou, Y. Chen, X. Wang, and Y. Ruan.Sedic: privacyaware data intensive computing on hybrid clouds. In Proceedings ofthe18th ACM conference on Computer and communications security, CCS’11, pages 515–526, New York, NY, USA, 2011. ACM.

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

[6]. R. D. Pietro and A. Sorniotti. Boosting efficiency and security in proof of ownership for deduplication. In H. Y. Youm and Y. Won, editors, ACM Symposium on Information, Computer and Communications Security, pages 81–82. ACM, 2012.

[7]. J. Li, X. Chen, M. Li, J. Li, P. Lee, andW. Lou. Secure deduplication with efficient and reliable convergent key management. In IEEE Transactions on Parallel and Distributed Systems, 2013.

[8]. R. D. Pietro and A. Sorniotti. Boosting efficiency and security in proof of ownership for deduplication. In H. Y. Youm and Y. Won, editors, ACM Symposium on Information, Computer and communications Security, pages 81–82. ACM.

[9]. M. Bellare, S. Keelveedhi, and T. Ristenpart.Dupless: Serveraided encryption for deduplicated storage. In USENIX Security Symposium, 2013.

Author’s Biography

M.Parabrahma rao *Dept.of computer science and Engineering,* srivenkateswara institute of technology *Kadapa-516001 A.P, INDIA*

Gunthati Prathap *Dept. of computer science andEngineering,* srivenkateswara institute of technology *Kadapa-516001 A.P, INDIA*