ISSN:0975-9646
Naveen. V et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (6) , 2016, 2531-2533

Providing Data Security to Files in Community and Hybrid Cloud

Naveen. V*
Assistant Professor/IT,
Kingston Engineering College

Naveen Kumar.J*
Assistant Professor/CSE,
Kingston Engineering College

Natteshan N.V.S*
Assistant Professor/CSE
Kingston Engineering College

Abstract— Cloud computing is the way of using cloud as a service for performing a computational task. There are different types of services which a cloud can provide like software as a service, platform as a service, infrastructure as a service. In this work a infrastructure as a service is used. Here files are stored effectively and in a secure manner by the help of Advanced Encryption Standard (AES) algorithm. Here there is usage of a community and hybrid cloud that is there is a public cloud and a private cloud. The public cloud is used for the purpose of storing of files. The private cloud is used for the purpose of providing the security to the file by the help of AES algorithm. There is also confidentiality and integrity is ensured in the files by the usage of encryption and decryption techniques. Thus a user can securely encrypt and decrypt a file and store it effectively.

Key words- Cloud computing, Advanced Encryption standard, Confidentiality, Integrity.

I. INTRODUCTION

Cloud computing is considered as a pay per usage service as provided by global leads like google, Amazon EC2 etc. and there are different types of cloud services like software as a service, Platform as a service and infrastructure as a service. In a software as a service a software is provided in a cloud where a user need not purchase the entire software and can use that software in a pay per usage basis. In a platform as a service a underlying platform like the operating system will be provided as a service. In a Infrastructure as a service a storage space is utilized in a pay per usage service. In this work Infrastructure as a service is utilized. Here a input file is given a normal id and then at the private cloud the encryption of the file will be done using the Advanced encryption standard and then the same file will be stored by the public cloud. When the user needs to download a file then the key must be provided to decrypt the file.

A. Purpose Of the research work

To effectively store the files in a cloud environment To utilize the effective combination of the hybrid cloud To perform the cryptographic techniques to the input file.

B. Objective of the work

To increase the security of download by using AES.
To provide confidentiality and integrity.
To enhance the effective storage of file.
The overall organization of this paper is as follows, section II gives the detail about the works related to this Secure file storage in cloud, section III gives the design of the system, section IV describes the experimental Setup and section V gives the evaluation of the experiments in a java environment, section VI concludes the work.

II. RELATED WORK

This section deals with the related work in the area of secure file storage in cloud environment.
Arthur rahumed et al. in their work, "A Secure Cloud Backup System with Assured Deletion and Version Control" proposes a secure cloud backup system that serves as a security layer on top of cloud storage services. It applies cryptographic protection to data backups.
Roxana Geambasu et al. in their work, "Keypad: An Auditing File System for Theft-Prone Devices" proposes an auditing file system for theft prone devices such as laptops and USB sticks. Key pad provides two important properties. First Key pad supports fine grained file auditing. Second a user can disable future file access after a device loss, even in the absence of device network connectivity. Keypad achieves these properties by weaving together encryption and remote key storage.
Sean quinlan et al. in their work, "Venti: A new approach to archival storage" describes a network storage system called venti which is used for archival data. In this system a unique hash of block's content act as a block identifier for read and write operations. It enforces a write-once policy preventing accidental or malicious destruction of data.
Yang tang et al. in their work, "FADE: Secure Overlay Cloud Storage with File Assured Deletion" designs FADE a practical, implementable and readily deployable cloud storage system that focuses on protecting deleted data with policy based file assured deletion. FADE is built upon standard cryptographic techniques such that it encrypts outsourced data files to make them unrecoverable to anyone upon revocation of file access policies.

III. APPROACH FOR SECURE UPLOADING AND DOWNLOADING OF FILES IN CLOUD

In this section the overall Architecture of the system will be explained

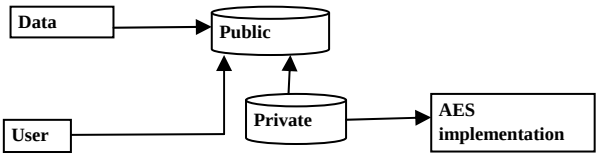

Fig.1 Overall Architecture Of Secure Storage In Cloud.

A. Description of the Overall Architecture

Here in this system a hybrid cloud is used. That is Both the public and private cloud. The private cloud is used for the generation of the secret key for both encryption and decryption purpose. The Public cloud is used for the purpose of storage of Files. Here the data owner is the

person who uploads the file. For this file a Encryption and key will be generated by the private cloud and this file is encrypted and is stored in the public cloud. Here a mechanism for checking the duplicate file is used. So this makes the storage of data more effective. Thereby reducing the storage space by avoiding redundant data. The user is the one who downloads the file when a download request is given by the user they should login by their account once if they login a Unique key value will be obtained which the user needs to supply to download that file. Thus it is assumed that there is a honest exchange of the key values between the private and public cloud without losing the confidentiality of the data. Thus because of the Encryption and decryption process of the Advanced Encryption technique a good level of security is achieved.

IV.Experimental Setup

The experiments were conducted by using a large input collection of files and the hybrid clouds are implemented as server programs and the user and the data owners are the client programs in java. The private cloud has a method to provide security by using the AES algorithm. If a data owner uploads a duplicate copy of the file it will not be uploaded and the user needs to provide the key value obtained from the private cloud to decrypt and utilize that file which he downloaded. These experiments were also conducted by using a single server program and the time to perform the encryption and decryption is found and the total users and the data owners and the cloud servers and the details of the file which are downloaded and the number of failures are found and are tabulated in the experimental evaluation section.

V.Experimental Evaluation And Analysis

There are various experiments conducted by using the input files and the effectiveness of this system is computed and the results obtained in the experiments are tabulated.
The number of Servers used and the clients and the number of files and their description is presented below,

Table I Description Of File

S NO	FILE NAME	FILE TYPE	FILE SIZE
1	Sample1.pdf	PDF	400Kb
2	Sample2.doc	DOC	77 Kb
3	Sample3.pdf	PDF	47 Kb
4	Sample4.ppt	PPT	400Kb
5	Sample5.docx	DOCX	47 Kb

The above table describes the details of the files along with the type of fiile and the size of the file

Table Ii System Constituents

No of severs	No of Data owners	No of users	No of files
3	50	85	400

The above table describes the details of the server, data owners, users and the files utilized

Table Iii Measure Of Values During The Process

No of Files Uploaded	No of Files Downloaded	No of Successful uploads	No of successful download	No of duplicate files
200	78	170	60	33

The above Table describes the details of the file downloaded and successful uploads and successful downloads performed and the number of duplicate files detected.

Table Iv Performance Time For Cloud Variants

SNO	FILE Name	Hybrid cloud Time	Single server Time
1	SAMPLE1.pdf	25 S	56 S
2	SAMPLE2.doc	35 S	40 S
3	SAMPLE3.ppt	40 S	60 S

VI.Conclusion And Future Research Scope

A effective storage of files is done in cloud and there is better security mechanism is provided by using the Advanced Encryption Standard algorithm. There is also a file level duplicate prevention which reduces the storage space and uses the available storage in a economical manner. There is also a performance measure comparison between the Hybrid cloud and the single server cloud is performed and it is found that the single server cloud is suffering from performance overheads and the level of confidentiality and the integrity can be observed by the failed downloads. The future scope for research can be in the secure cryptographic algorithm used and the way in which the duplicate file is found can be done even in block level by parsing the input strings in the input file and prevent duplication.
The above table describes the time and the processing overhead of bith Hybrid cloud and single server cloud.

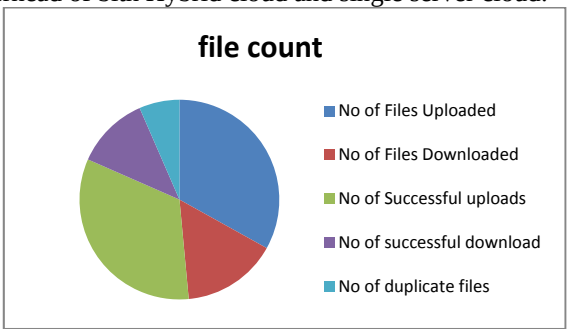

Fig. 2 File Download and Upload details

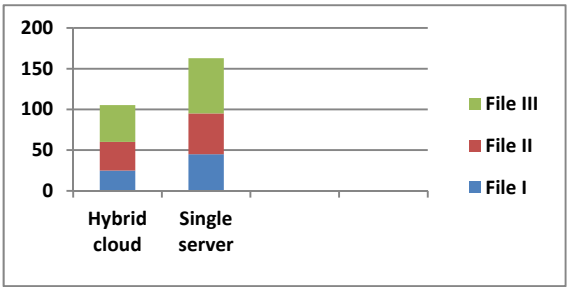

Fig. 3. Processing time comparison between hybrid and single server Cloud

VI. Conclusion And Future Research Scope

A effective storage of files is done in cloud and there is better security mechanism is provided by using the Advanced Encryption Standard algorithm. There is also a file level duplicate prevention which reduces the storage space and uses the available storage in a economical manner. There is also a performance measure comparison between the Hybrid cloud and the single server cloud is performed and it is found that the single server cloud is suffering from performance overheads and the level of confidentiality and the integrity can be observed by the failed downloads. The future scope for research can be in the secure cryptographic algorithm used and the way in which the duplicate file is found can be done even in block level by parsing the input strings in the input file and prevent duplication.

References

[1] Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P.C. Lee, and Wenjing Lou, "A Hybrid Cloud Approach for Secure Authorized Deduplication", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 5, MAY 2015.

[2] P. Anderson and L. Zhang, "Fast and secure laptop backups with encrypted de-duplication," in Proc. 24th Int. Conf. Large Installation Syst. Admin., 2010, pp. 29–40.

[3] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-locked encryption and secure deduplication," in Proc.32nd Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2013, pp. 296–312.

[4] 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.

[5] M. Bellare and A. Palacio, "Gq and schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks," in Proc. 22nd Annu. Int. Cryptol. Conf. Adv. Cryptol., 2002, pp. 162–177.

[6] 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.

[7] M. W. Storer, K. Greenan, D. D. E. Long, and E. L. Miller, "Secure data deduplication," in Proc. 4th ACM Int.Workshop Storage Security Survivability, 2008, pp. 1–10

[8] A. Rahumed, H. C. H. Chen, Y. Tang, P. P. C. Lee, and J. C. S. Lui, "A secure cloud backup system with assured deletion and version control," in Proc. 3rd Int. Workshop Secutiry Cloud Comput., 2011, pp. 160–167.

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