ISSN (ONLINE):2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.25, February 2017

Efficient Data Storage Security and Services in Cloud Computing Environment with Security Principles Algorithm

[1]J.Velmurugan, [2]S.K. Manigandan, [3] P.Vinothkumar
[1, 2, 3] Asst.Prof. Department of Information Technology,
[1, 2, 3] Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai, India

ABSTRACT:

The number of cloud users and the amount of sensitive data on cloud is increasing massively, so there is a serious need to provide security to the data stored in cloud. Cloud computing allows the user to store the massive amount of data in cloud and to make use of it on demand. One of the greatest challenges in cloud is data security. Since there is a serious security issue in cloud, users are more concerned about the sensitive data, which they store in cloud. Thus to implement the strong security to the data stored in cloud, we can directly forwards the message through storage server from one user to the another user.A decentralized erasure code is an erasure code that independently computes each codeword symbol for a message. The scheme steganography is used, thereby hiding the sensitive data within the images. All these techniques are collaborated together, to implement strong security to the issues made to the data, which we store in cloud.

KEYWORDS: Storage Server, Data Forwarding, Erasure code, Data Integrity, steganography

1. INTRODUCTION

Cloud computing is the trending technology which provides services via the internet. It is on demand delivery of IT resources via internet with the concept of pay-on-demand. The important service provided by the cloud computing is cloud storage, which makes it possible for the cloud users to move their data to the cloud. But due to the untrusted cloud server, the cloud users are worrying about the data, they store in cloud. Since the data storage location is virtual to them. Data robustness is a major requirement for storage systems. There have been many proposals of storing data over storage servers. One way to provide data robustness is to replicate a message such that each storage server stores a copy of the message. It is very robust because the message can be retrieved as long as one storage server survives.

Another way is to encode a message of k symbols into a codeword of n symbols by erasure coding. To store a message, each of its codeword symbols is stored in a different storage server. A storage server failure corresponds to an erasure error of the codeword symbol. As long as the number of failure servers is under the tolerance threshold of the erasure code, the message can be recovered from the codeword symbols stored in the available storage servers by the decoding process. This provides a tradeoff between the storage size and the tolerance threshold of failure servers.

A decentralized erasure code is an erasure code that independently computes each codeword symbol for a message. Thus, the encoding process for a message can be split into n parallel tasks of generating codeword symbols. A decentralized erasure code is suitable for use in a distributed storage system. After the message symbols are sent to storage servers, each storage server independently computes a codeword symbol for the received message symbols and stores it. This finishes the encoding and storing process. The recovery process is the same.

2. EXISTING SYSTEM

In recent years, resources such as text data, images etc. are delivered as services in cloud computing. Due to the high speed network performance of cloud computing, user can access these resources from any part of the world. Cloud storage is considered to be a collection of storage servers. The data confidentiality in cloud servers are at risk, since data are uploaded into a third party cloud system [1].Thus a secure storage system is built by integrating threshold proxy re-encryption scheme and decentralized erasure code. These schemes not only propose a robust way of storing and retrieving confidential data but also introduce data forwarding mechanism. In this mechanism, data owner can command the storage server to forward the encrypted data to another user by Threshold proxy re-encryption scheme. They performs encoding operation of the encrypted data and forwards the encoded data to another requested user. Decentralized erasure code scheme encodes message of K symbols into codeword of ‘n’ symbols and store these code word into different storage servers. These messages can be retrieved even one server fails to respond. But it fails to identify the storage server which tries to modify the data stored in it. i.e., lack of data error localization mechanism and dynamic data support. Client has no physical control over the data which is outsourced into the cloud. Therefore a new security risk is developed towards accuracy of data in cloud and data confidentiality becomes a serious concern. Encoded messages are distributed as code symbols, encrypted and stored in cloud servers.

3. PROPOSED WORK

In proposed work, addressing a problem of forwarding, a data from one user to another by storage servers is directly under the command of the data owner, along with an effective distributed data verification and data retrieval mechanism is implemented. It provides assurance to the integrity and availability of the data uploaded into the cloud. The uploaded data is divided into blocks and stored in different servers. By this data availability can be assured using erasure correction code. The algebraic property of erasure code helps to retrieve the lost or modified data. Unreliable servers which perform these data block modifications are identified by holomorphic tokens by using challenge response auditing mechanism. Third Party Auditor (TPA) performs this data error localization process i.e., identification of misbehaving servers. The client’s uploaded data will be encrypted by the cloud server and this prevents TPA from accessing the data. It also supports dynamic data support including block update, delete and append.

SECURE DATA STORAGE IN CLOUD

In cloud data storage system, users store their data in the cloud and no longer possess the data locally. Thus, the correctness and availability of the data files being stored on the distributed cloud servers must be guaranteed. One of the key issues is to effectively detect any unauthorized data modification and corruption, possibly due to server compromise and/or random Byzantine failures. Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance, since it can be the first step to fast recover the storage errors. To address these problems, our main scheme for ensuring cloud data storage is presented in this section. The first part of the section is devoted to a review of basic tools from coding theory that is needed in our scheme for file distribution across cloud servers. This can be perfectly integrated with the verification of erasure-coded data. Subsequently, it is also shown how to derive a challenge response protocol for verifying the storage correctness as well as identifying misbehaving servers. Finally, the procedure for file retrieval and error recovery based on erasure-correcting code is outlined.

IMPLEMENTATION OF ERASURE CORRECTION CODE

File F can be distributed into several data blocks and each data blocks are generally stored in separate cloud and replica servers. Data blocks could be modified by any unreliable servers through external or internal attacks. If many data block is lost or modified then it can be retrieved from the corresponding replica server. Data blocks could not be recovered back if any malfunction in replica server is observed. To overcome this constrain in replica servers, an algebraic property called Erasure Correction Code is used. To recover the modified or lost data block it requires the coordination of all the servers where F's data blocks are stored.

If the data block corruption have been detected in r rows, download all the data blocks present in that row. Let s denote the number of misbehaving or unreliable servers and k denotes the total number of servers. The s servers should be treated as the erasures and the lost data could be extracted from other servers. This can be possible only when $s \leq k$. If this condition fails due to redundancy there will be no chance to recover the corrupted block even if the position of the unreliable file is known. Once the data is recovered it must be sent to the corresponding servers which caused the data block modifications. Our data storage correctness verification scheme is based on random spot checking. Depending on the parameters like r, l and t higher probability of successful file recovery can be assured.

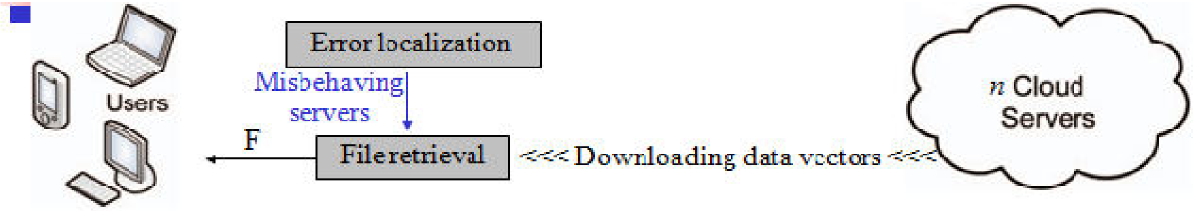

Figure 1: Erasure Code Implementation

4. SYSTEM ARCHITECTURE

In the following diagram, the proposed architecture consists of a multiple users, multiple storage servers which store the keys and data separately, and an application which manages key generation as well management. They work independently. Our system provide multiple encryption to safeguard the data effectively. Apart from storage, the data is forwarded to other user access by means of encryption where the data is decrypted and encrypted for the use of the other user.

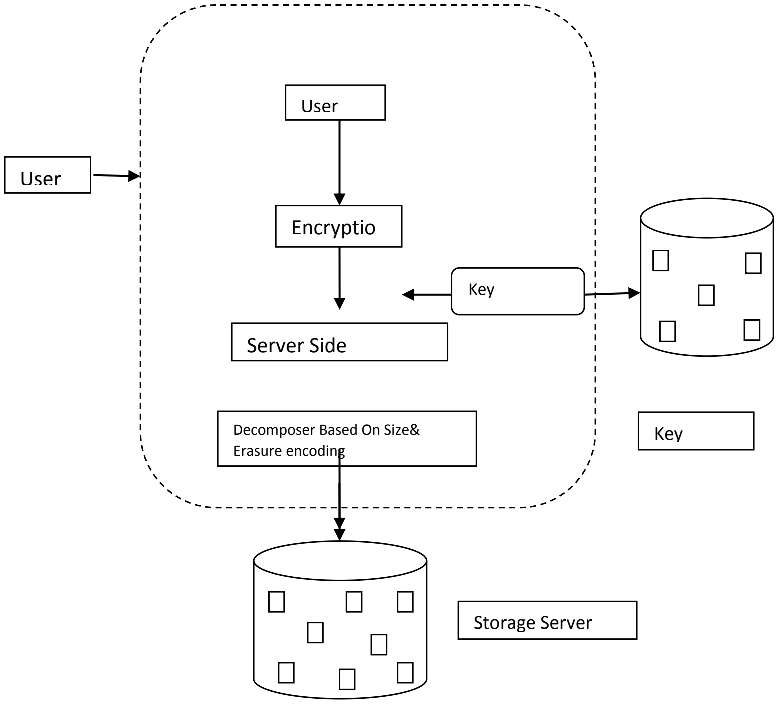

Figure 2: Architecture of the proposed system

5. PERFORMANCE ANALYSIS:

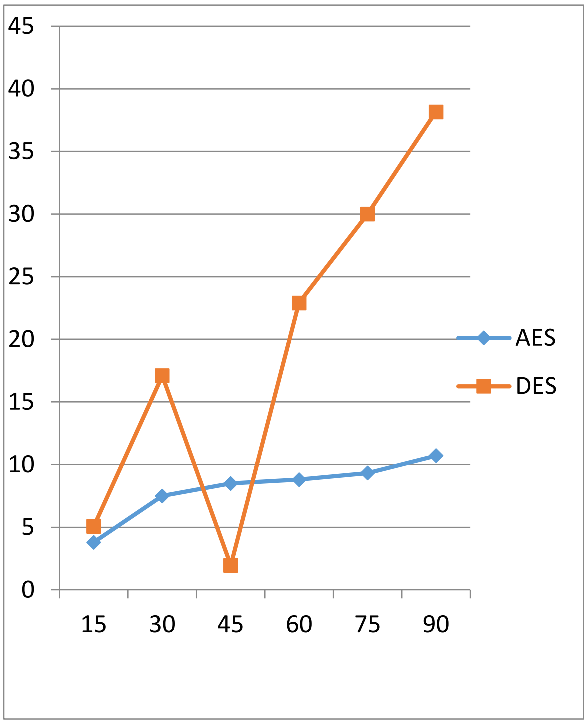

Figure **3** Encryption time for Erasure code code with current data

Input size in KB	Erasure Code	Current Data
15	3.8	5.07
30	7.5	17.09
45	8.5	1.96
60	8.8	22.91
75	9.33	29.99
90	10.7	38.15
Time taken	8.105	22.195

Table 1 Encryption time taken by Erasure with current data

6. CONCLUSION:

By this project, we successfully achieved our objective to store the data securely in the cloud. Also we have proposed an approach that ensures the security principles such as confidentiality and integrity of data in cloud. The major analysis made in this paper is that, how to secure the data from an unauthorized access. By our proposal system, we achieved to get 98% data security approximately. The serious data security issue can be compromised by using enhanced encryption algorithms.

REFERENCES:

[1] Deepanchakaravarthi Purushothaman and Dr.Sunitha Babura, “An Approach for Data Storage Security in Cloud Computing”, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012.

[2] Sumeena R and Dr. H S Guru Prasad, "Effective Secure Storage and Retrieve In Cloud Computing"IRACST - International Journal of Advanced Computing, Engineering and Application (IJACEA), ISSN: 2319-281X, Vol. 3, No.3, and June 2014.

[3] Poona M. Pradesh and Proof Bharat Tide," Improving Data Integrity for Data Storage Security. In Cloud Computing", Poona M. Pardeshietal, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5), 2014, 6680-6685.

[4] Urinal Kant Sarkar and Trait Chatterjee,"Enhancing data storage security in cloud computing through steganography" ACEEE nit's on Network security, vol.5, NO.1, January 2014.

[5] J.Vemurugan "Enhancing the Data Storage Security in Cloud Computing With Cryptography Security Principles" International Journal for Scientific Research & Development (IJSRD) Volume 4, Issue 1, March 2016 – ISSN: 23210613.

[6] J.Velmurugan "A Novel Approach for Security Enhancement and Efficient Data Recovery in Cloud Computing" International Journal of Scientific and Engineering Research (IJSER) Paper ISSN 2229-5518 Volume 7, Issue 4, April 2016.

[7] Miss. Nucor M. Yaw ale and Proof V. B. Gadichha,"Third Party Auditing (TPA) for Data Storage Security in Cloud "International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013.