Scientific Journal of Impact Factor(SJIF): 3.134

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 4, April -2015

# ASSURING SECURED AND DEPENDABLE CLOUD STORAGE WITH ERASURE CODE AND TPA MANAGEMENT SYSTEM

MS. TINTU BABU[1], PROF. M.BABU[2]

[1]Computer Science And Engineering,Gkm College Of Engineering And Technology, Chennai, India
[2]Computer Science And Engineering,Gkm College Of Engineering And Technology
Chennai, India

***Abstract***— *The cloud computing is a technology which provides various services through internet. There is no big security provided in the cloud server for data safety. In this project, cloud server spilt the file into batches and allowed for encryption. These encrypted batches are kept in replica servers as a backup. This encrypted data are converted into bytes and added parity bit process by the data owner in order to restrict TPA by accessing the original data. The cloud server generates the token number from the parity added encrypted data and compared with the signature provided to the TPA to verify the data integrity. The erasure code is implemented for the back-up of the data. The encryption process of the data is done by the data owner before it reaches the cloud server. This ensures proper double time security.*

***Keywords***—*Encryption, Replica, TPA, Erasure code*

## I. INTRODUCTION

Several trends are opening up the era of cloud computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the Software as a Service (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centers.

In order to achieve the assurances of cloud data integrity and availability and enforce the quality of cloud storage service, efficient methods that enable on-demand data correctness verification on behalf of cloud users have to be designed. However, the fact that users no longer have physical possession of data in the cloud prohibits the direct adoption of traditional cryptographic primitives for the purpose of data integrity protection.

Hence, the verification of cloud storage correctness must be conducted without explicit knowledge of the whole data files, Meanwhile, cloud storage is not just a third party data warehouse. The data stored in the cloud may not only be accessed but also be frequently updated by the users, including insertion, deletion, modification, appending, etc. Thus, it is also imperative to support the integration of this dynamic feature into the cloud storage correctness assurance, which makes the system design even more challenging. Last but not the least, the deployment of cloud computing is powered by data centers running in a simultaneous, cooperated, and distributed manner. It is more advantages for individual users to store their data redundantly across multiple physical servers so as to reduce the data integrity and availability threats. Thus, distributed protocols for storage correctness assurance will be of most importance in achieving robust and secure cloud storage systems. However, such important area remains to be fully explored in the literature.

### PROBLEM STATEMENT

Constructing a secure storage system that supports multiple functions is challenging when the storage system is distributed and Storing data in a third party's cloud system causes serious concern on data confidentiality.

### MOTIVATION

There is no big security provided in the Cloud server for data safety. If at all security exists, the third party auditor should be allowed to access the entire data packets for verification and there is no backup process. To protect outsourced data in cloud storage against corruptions, adding fault tolerance to cloud storage, along with efficient data integrity checking and recovery procedures.

## II. EXISTING SYSTEM

In the existing system, there is no big security provided in the Cloud server for data safety. Only single server used for storing data. So single point failure occurred. That is failure to any data in a single server affect the whole system. Therefore all data loss from the server. After using multiple server this problem could be avoided.

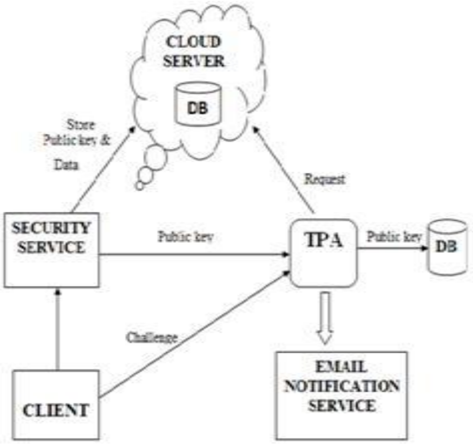

Fig1: Cloud Architecture

The encryption schemes in the existing system are not effective because only few operations are supported over encrypted data. If at all security exists, the third party auditor should be allowed to access the entire data packets for verification. cloud suffers from a permanent failure and loses all its data There is no effective backup process in the existing system.

## III. PROPOSED SYSTEM

In the proposed system, Cloud server will spilt the file into batches and allowed for encryption. The corresponding encrypted batches are kept in different Cloud servers and their keys are distributed in different key server. This encrypted data are converted into bytes and added parity bit process by the data owner in order to restrict TPA by accessing the original data. The Cloud server generates the token number from the parity added encrypted data and compared with the signature provided to the TPA to verify the Data Integrity. Also implement Erasure Code for the back-up of the data. The encryption process of the data by the data owner done before it reaches the Cloud server. This ensures proper double time security.

ADVANTAGES

□ One way to provide data robustness is to replicate a message such that each storage server stores a copy of the message.

□ A decentralized erasure code is suitable for use in a distributed storage system.

□ A re-encryption scheme and integrate it with a secure decentralized code to form a secure distributed storage system is proposed.

□ The encryption scheme supports encoding operations over encrypted messages and forwarding operations over encrypted and encoded messages.

□ The tight integration of encoding, encryption, and forwarding makes the storage system efficiently meet the requirements of data robustness, data confidentiality, and data forwarding.

## IV. ARCHITECTURE

DATA OWNER

To upload the data into the Cloud server, the Data Owner have be registered in the Cloud Server. Once the Data Owner registered in cloud server, the space will be allotted to the Data Owner. Owner is the Person who is going to upload the data in the Cloud Server.

MAIN CLOUD SERVER

The cloud server where data being stored and accessed by cloud data owner or users. Data should not be accessed by unauthorized users, no data modification or no loss of data.

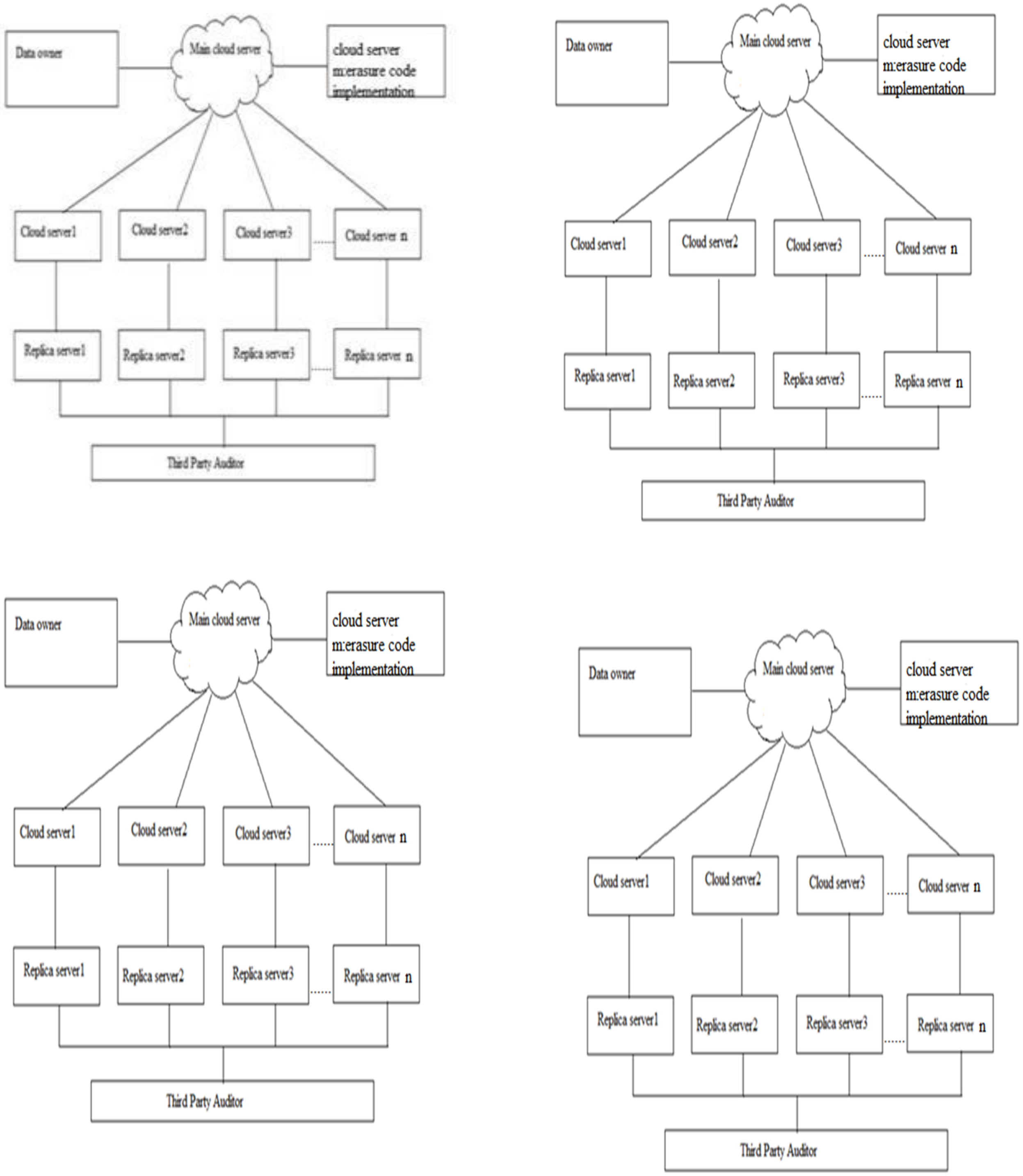

Fig2:Architect

Cloud Server is the area where the user going to request the data and also the data owner will upload their data. Once the user send the request regarding the data they want, the request will first send to the Cloud Server and the Cloud Server will forward your request to the data owner. The data Owner will send the data the data the user via Cloud Server. The Cloud Server will also maintain the Data owner and Users information in their Database for future purpose.

REPLICA SERVER

If suppose the data in the data server was lost, then the main cloud server will contact the replica cloud server and get the data from the replica cloud server.

### TRUSTED PARTY AUDITOR

TPA performs reviews for multiple clients simultaneous and efficient. Extends security and performance analysis demonstrate the proposed framework are provably secured and very effective. To securely introduce a powerful trusted party auditor (TPA), the accompanying two essential prerequisites must be

□ TPA should be able to effectively audit the cloud information storage without requesting the neighbourhood duplicate of data, and present no extra on-line burden to the cloud client;

□ The third party auditing procedure should to acquire no new vulnerabilities towards client data privacy.

### ERASURE CODE

Erasure code is used for recovering the lost data by using XOR operation, while XORing the block data , the data will be converted in binary data.

## V. ALGORITHMS

### 1.ADVANCED ENCRYPTION STANDARD

AES is a block cipher with a block length of 128 bits. AES allows for three different key lengths: 128, 192, or 256 bits. Encryption consists of 10 rounds of processing for 128-bit keys,12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Except for the last round in each case, all other rounds are identical. Each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key.

The order in which these four steps are executed is different for encryption and decryption. To appreciate the processing steps used in a single round, it is best to think of a 128-bit block as consisting of a 4×4 matrix of bytes. Therefore, the first four bytes of a 128-bit input block occupy the first column in the 4 × 4 matrix of bytes. The next four bytes occupy the second column, and so on. The 4 × 4 matrix of bytes is referred to as the state array. AES also has the notion of a word. A word consists of four bytes, that is 32 bits.

Therefore, each column of the state array is a word, as is each row. Each round of processing works on the input state array and produces an output state array.The output state array produced by the last round is rearranged into a 128-bit output block.

### 2.ERASURE CODE

Erasure coding is a method of data protection in which data is broken into fragments, expanded and encoded with redundant data pieces and stored across a set of different locations or storage media.The goal of erasure coding is to enable data that becomes corrupted at some point in the disk storage process to be reconstructed by using information about the data that's stored elsewhere in the array. Erasure codes are often used instead of traditional RAID because of their ability to reduce the time and overhead required to reconstruct data. The drawback of erasure coding is that it can be more CPU-intensive, and that can translate into increased latency.

## VI. CONCLUSION

In this project, problem of data security in cloud data storage was investigated, which is essentially a distributed storage system. To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users, an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append proposed. erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability. By utilizing the homomorphic token with distributed verification of erasure coded data, our scheme achieves the simultaneous identification of the misbehaving server(s).

## REFERENCES

[1] Henry C.H. Chen and Patrick P.C. Lee “Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage: Theory and Implementation” ieee transactions on parallel and distributed systems, VOL. 25, NO. 2, february 2014.

[2] Almas Ansari, Prof.Chetan Bawankar, “ Privacy & data integrity for secure cloud storage,” IOSR Journal of Computer Science (IOSR-JCE)

[3] Giuseppe Ateniese “Remote Data Checking Using Provable Data Possession” ACM Transactions on Information and System Security, Vol. 14, No. 1, Article 12, Publication date: May 2011.

[4] Hemalata A. Gosavi , Prof. Manish R. Umale "Public Auditing and Data Dynamics for Storage Security in Cloud Computing" International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 4 - May 2014.

[5] Hussam Abu-Libdeh and Hakim Weatherspoon "RACS: A Case for Cloud Storage Diversity", June 10–11, 2010, Indianapolis, Indiana, USA.Copyright

[6] K.Adhiyaman, A. Jesudoss, D.Saravanan "Trusted Public Auditing Process for Secure Cloud Storage" IPASJ International Journal of Information Technology Volume 2, Issue 3, March 2014.

[7] Ms. Shweta khidrapure1 and Prof. Archana lomte "Blinear pairing based public auditing for secure cloud storage using TPA (IJAIEM) Volume 3, Issue 7, July 2014.

[8] Tejashree Paigude#, Prof. T. A. Chavan "A survey on Privacy Preserving Public Auditing for Data Storage Security" International Journal of Computer Trends and Technology " volume4 Issue3- 2013.

[9] M.Yugandhar, D. Subhramanya Sharma " Security of Data Dynamics in Cloud Computing" International Journal of Computer Science and Information Technologies, Vol. 3 (4) , 2012,4868-4873.

[10] Nupoor M. Yawale Prof. V. B. Gadichha " Third Party Auditing (TPA) for Data Storage Security in Cloud with RC5 Algorithm" International Journal of Advanced Research Volume 3, Issue 11, November 2013.