International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.2, No.4, April 2013 DOI:10.15693/ijaist/2013.v2i4.106-110

# A Survey of the Research on Future an Error Identify and Error Correction

**Vijayaraghavan, U*., Madonna Arieth, R!., and ¶R.Anand Babu.**

*! Asst.Professor, Department of Computer Science and Engineering, RVS College of Engineering & Technology, Karaikal.
¶ Asst.Professor, Department of Information Technology, RVS College of Engineering & Technology, Karaikal.

***Abstract***

***In this paper, an error recovery and error correction analysis is used for to this secure computing process. In this contrast to the traditional solutions, where IT services are under proper physical, logical and personnel controls, cloud computing moves to the applications software and databases for the large data centers. In the managing of data and services may not be fully trustworthy and which inevitably poses new security risks toward the correctness of data in this cloud computing. In propose work, error identification of misbehaving server(s), error correction process and update the error data file to using the cloud trust computing security process.***

**Key Words:** Cloud computing, Error localization, Error Update Algorithm, data dynamics, High-Availability and Integrity Layer, Proof of retrievability (POR),

## 1 INTRODUCTION

### 1.1 Cloud Computing Services

Several trends are opening up the area 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.

Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) [1] are both well known examples. Cong Wang et.al [2] has proposed while these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data. Recent downtime of Amazon's S3 is such an example.

### 1.2 Third Parity Auditor

Cong Wang et.al [2] suggests in order saving the time, computation resources, and even the related online burden of users, we also provide the extension of the proposed main scheme to support third-party auditing, where users can safely delegate the integrity checking tasks to third-party auditors (TPA) and are worry-free to use the cloud storage services. Our work is among the first few ones in this field to consider distributed data storage security in cloud computing.

Our contribution can be summarized as the following three aspects:

1) Compared to many of its predecessors, which only provide binary results about the storage status across the distributed servers, the proposed scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server (s).

2) Unlike most prior works for ensuring remote data integrity, the new scheme further supports secure and efficient dynamic operations on data blocks, including: update, delete, and append.

3) The experiment results demonstrate the proposed scheme is highly efficient. Extensive security analysis shows our scheme is resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

## 2 KEY RESEARCH TOPICS

### 2.1 Environment Work Survey

Kervin.D et.al [3] has proposed explore a unification of the two approaches to remote file-integrity assurance in a system that we call HAIL (High- Availability and Integrity Layer). HAIL manages file integrity and availability across a collection of servers or independent storage services. It makes use of PORs as building blocks by which storage resources can be tested and reallocated when failures are detected. HAIL does so in a way that transcends the basic single-server

design of PORs and instead exploits both within-server redundancy and cross-server redundancy. HAIL relies on a single trusted verifier—e.g., a client or a service acting on behalf of a client—that interacts with servers to verify the integrity of stored files HAIL offers the following benefits: Strong file-intactness assurance: HAIL enables a set of servers to prove to a client in challenge-response protocol that a stored file is fully intact—more precisely, that the client can recover file with overwhelming probability. HAIL protects against even small, e.g., single-bit, changes to file.

### 2.1.1 Message Authentication Code (MAC)

Kervin.D et.al [3] suggests MAC is appended to a message .Our goal in this section is to define a cryptographic primitive that acts both as a MAC and an error correcting (or reassure) code. Moreover, we leverage the redundancy added by the error –corre code for constructing the MAC. Such a primitive allows efficient checking of server response in our HAIL protocol.

**MAC Procedure:**

1. /* output F*/
F←---- (Input U1, Output V2)
2. /* Compute File Share */
Server ←-----(S1,S2,S3)
3. /* generate nq challenge*/
For j=1 to no do
4. /* Challenge all servers
for a=1 to nq do
5. /* A responds for if j,f then Corrected servers */
S corr ←------S corr U (j)
6. /* Sj,S in correct replies blow q*/
if denote-F(output V2,Input U1)
7. /*F Error File can be recovered
else output 1
8. /* F is Corrupted*/.

### 2.1.2 Proof of Retrivability (POR)

Ari Juels [4] has proposed a Proof of retrievability (POR) is a compact proof by a file system (prover) to a client (verifier) that a target file F is intact, in the sense that the client can fully recover it. As PORs incur lower communication complexity that transmission of F itself, they are an attractive building block for high assurance remote storage system.

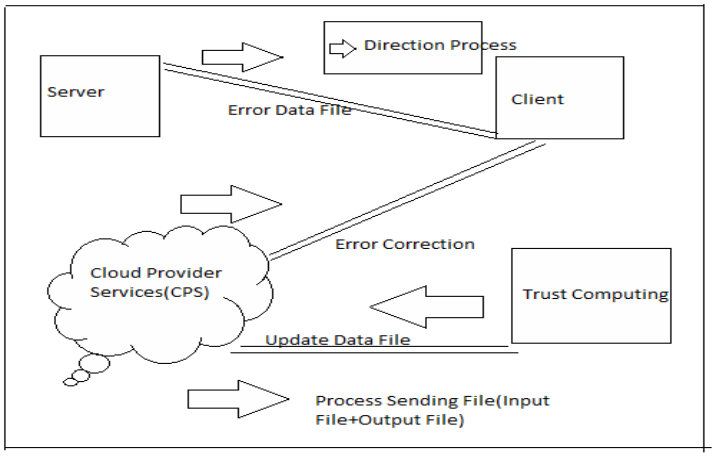



**Fig: 2.1.2.1** Proof of Retrievability Data flow Diagram

## 3 RESEARCH EXISTING SYSTEM WORK

### 3.1 Existing system process

Krin Kumar.K et.al [5] Suggests previous system proposed that a public auditing scheme consists of four algorithms (Key Gen, Sig Gen, Gen Proof, Very Proof). Key Gen is a key generation algorithm that is run by the user to setup the scheme. Sig Gen is used by the user to generate verification metadata, which may consist of MAC, signature, or other related information that will be used for auditing. Gen Proof is run by the cloud server to generate a proof of data storage correctness, while verify proof is run by the TPA to audit the proof from the cloud server. Public auditing system can be constructed from the auditing scheme in two phases, setup and audit. Our proposed system enable privacy –preserving public auditing for cloud data storage under a fore mentioned model. Our protocol design should achieve the following security and performance guarantee:

**1. Public Audit ability**

To allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional on-line burden to the cloud users.

**2. Storage Correctness**

To ensure that there exists no checking cloud server that can pass the audit from TPA without indeed storing user data intact.

**3. Privacy-Preserving**

To ensure that there exists no way for TPA to derive users data content from the information collected during the auditing process.

**4. Batch Auditing**

To enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously.

**5. Lightweight**

To allow TPA to perform auditing with minimum communication and computation overhead.

## 4 RESEARCH PROPOSE WORK PROCESS

### 4.1 Design system process

A. Storage correctness.
B. Fast localization of data error.
C. Dynamic data support.
D. Constancy
E. Inconsequential.

**A. Storage correctness**

To ensure users that their data are indeed stored appropriately and kept intact all the time in the cloud.

**B. Fast localization of data error**

To effectively locate the malfunctioning server when data corruption has been detected.

**C. Dynamic data support**

To maintain the same level of storage correctness assurance even if users modify, delete, or append their data files in the cloud.

**D. Constancy**

To enhance data availability against Byzantine failures, malicious data modification and server colluding attacks, i.e., minimizing the effect brought by data errors or server failures.

**E. Inconsequential.**

To enable users to perform storage correctness checks with minimum overhead.

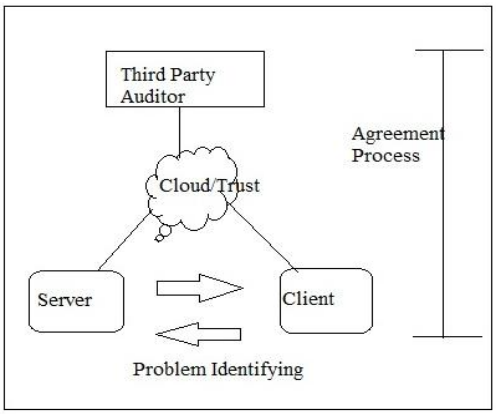



**Fig: 2.1.2.1** Cloud Agreement Architecture

## 5 EXPERIMENT RESULT

We now assess the performance of the proposed third parity auditor and privacy-preserving public auditing scheme. We will focus on the extra cost, error update process, and the efficiency of the error recovery cloud computing process. The proposed system outperforms with compares large data centers to the previous system, which gives an optimal result.

The following figure illustrates the compassion result and shows the best result.

- **Error Identify S1**

The service providers an error identify the data error file (S1).

- **Error Correction S2**

To service provider the third parity auditor (TPA) using the data error correction (S2).

- **Update File S3**

To service provider the trust computing using an update file. In intimation to server message (S1+S2=S3) Services.

### 5.1 Error Update Algorithm

**Algorithm: Generation for Error Recovery Process**:
**Input: A Set of Data U1**
**Output: A Set of Error update process V2**
1. For each U1=V2
2. Se--→ Data Loss;
3. For each S←--- Se do
4. / Se Analysis the Error Data S*/
5. if Se ---→S1 (U1.V2) then
6. S 2←------Error Correction Data File(S/Se);
7. / Update Data file S3(U1,V2) S*/
8. else if Se---→S1(U1,V2);
9. S←-------Se to send the Update file
10. End.

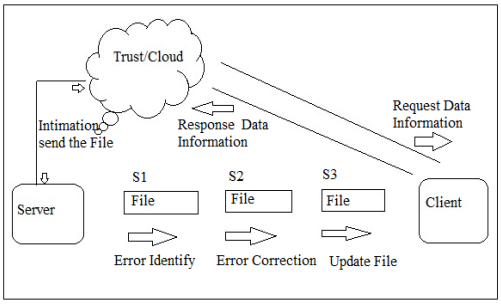
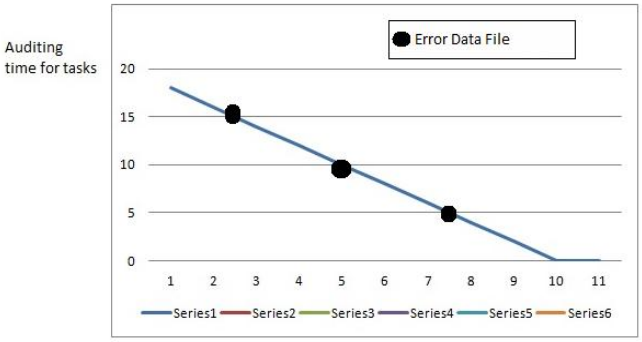



**Fig: 5.1.1** Error Recovery Cloud Computing Process.




**5.2 Experimental Chart work**

**Fig: 5.2.1** Number of Auditing tasks pervious system

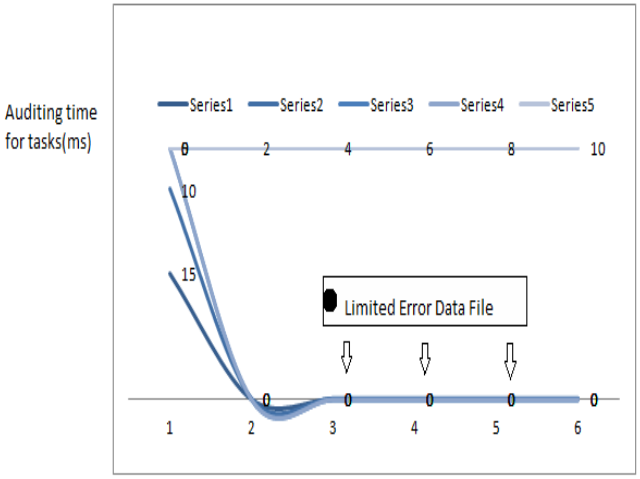



**Fig: 5.2.2** Number of Auditing tasks propose system

**Acknowledgements**

I wish to express my warmest, sincerest thanks and deepest gratitude to my Research advisor, Prof.Dr.R.KANTHAVEL,M.E.,Ph.D., Department of Electronics and Communication Engineering, Velammal Engineering College, Chennai., for her impeccable guidance, numerous opportunities and valuable suggestion for my research work. I would like to thank Assit.Professor Dr.A.RAJARAM,M.E.,Ph.D., Department of Electronics and Communication Engineering, Karphagam College of Engineering, Coimbatore., for his valuable suggestions in my scientific endeavors. I would like to thank my Prof.Dr.B.NAGALINGESWARAJU,M.Tech.,Ph.D., Principal, RVS College of Engineering and Technology, Karaikal.

**References**

[1] Amazon.com. "Amazon web service (aws)," Online at http://aws.amazon.com/2009.

[2] Cong Wang, Qian Wang, Kui Ren, Ning Cao and Wenjing, (2012) "Towared secure and Dependable storage service in cloud computing", IEEE.

[3] Kervin. D, Bowers, Ari Juels and Alina Opera, (2009) "HAIL:-Availability and Integrity Layer for Cloud Storage", IEEE.

[4] Ari Juels, Burton and Kaliski.S., (2007) "Proofs of Retrivability for large files", IEEE/2007.

[5] Krin Kumar. K, Padmaja.K and Radha Krishna. P., (2012) "Automatic Protocol Blocker for Privacy-Preserving Public Auditing in Cloud Computing" Transaction on cloud Computing, Volume: PP, Issue: 99. www.Chennaisunday.com.

**Author Profile**

Mr.U.Vijayaraghavan received the B.Tech degree in Information & Technology from the Lord Venkateshwarra Engineering College, Kanchipuram (Anna University Chennai), Tamil Nadu, India. He earned M.E Computer Science & Engineering in Anna University, Coimbatore, Academic Campus, India. He is a member of IAENG. He published papers in International and National level conference. He is working as a Lecture in Dept of Information Technology, Lord Venkateshwaraa Engineering College, Kanchipuram. Currently he is working as an Assistant Professor in the Department of Computer Science and Engineering, RVS College of Engineering &Technology, Karaikal, Puducherry, India. His Research interest includes Cloud Computing, Grid Computing and Optical Networks.

Mrs.R.Madonna Arieth received the M.Sc degree in Information & Technology from Bhrathidasan University, Trichy.She earned M.Tech Computer Science & Engineering in Prist University, Thanjavour, India. She is working as a Asst.Professor in

RVS College of Engineering &Technology, Karaikal, Puducherry, India.His area of research is Cloud Computing and Computer networks.

Mr.R.Anand Babu received the B.Tech degree in Information Technology from the E.G.S.Pillay Engineering College, Nagapattinam, TamilNadu, India.He is Completed M.Tech Computer Science &Engineering in Prist niversity, Thanjavour, India. Currently he is working as a Assistant Professor in RVS College of Engineering &Technology, Karaikal, Puducherry, India. His research interest includes Grid Computing & Computer networks.