IOSR Journal of Engineering (IOSRJEN)
e-ISSN: 2250-3021, **p**-ISSN: 2278-8719
Vol. 3, Issue 8 (August. 2013), ||V2|| PP 01-05

Near Sheltered and Loyal storage Space Navigating in Cloud

N.Venkata Krishna, M.Venkata Ramana
1. M.Tech student, 2. Assistant Professor
Global College of Engineering And Technology, Kadapa

Abstract: - Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks towards the correctness of the data in cloud. Prior work has addressed this problem using either public key cryptography or requiring the client to outsource its data in encrypted form. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. In this paper we introduce a technique called auditing, which is done by a person called third party auditor (TPA).

I. INTRODUCTION

In recent years, the concept of third-party data warehousing and, more generally, data outsourcing has become quite popular. Appealing features of outsourcing include reduced costs from savings in storage, maintenance and personnel as well as increased availability and transparent up-keep of data. At the same time, though, such services eliminate the direct oversight of component reliability and security that enterprises and other users with high service-level requirements have traditionally expected.

In this paper, we propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud. We rely on erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability. Our proposed solution to provide storage service accountability is through independent, third party auditing and arbitration. The TPA is the crucial person here for accepting the data to upload the data into cloud server. 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.

Third-party auditing is an accepted method for establishing trust between two parties with potentially different incentives. Auditors assess and expose risk, enabling customers to choose rationally between competing services. More recently, however, the problem of Provable Data Possession (PDP) –is also sometimes referred to as Proof of Data Retrivability (POR)– has popped up in the research literature. The central goal in PDP is to allow a client to efficiently, frequently and securely verify that a server – who purportedly stores client's potentially very large amount of data – is not cheating the client.

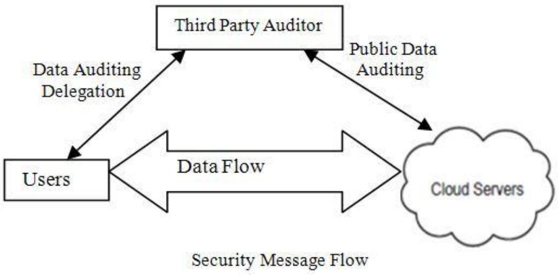
It manages file integrity and availability across a collection of servers or independent storage services. It makes use of PORs as building blocks by which storage resources can be tested and reallocated when failures are detected. In order to achieve the assurances of cloud data integrity and availability 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.

In this paper, we propose an effective and flexible distributed storage verification scheme with explicit dynamic data support to ensure the correctness and availability of users' data in the cloud. A POR uses file redundancy within a server for verification. In a second, complementary approach, researchers have proposed distributed protocols that rely on queries across servers to check file availability. To restore security assurances eroded by cloud environments, researchers have proposed two basic approaches to client verification of file availability and integrity.

II. PROBLEM STATEMENT

Mostly cloud data storage service involving three different entities, as illustrated in Fig. 1: the cloud user, who has large amount of data files to be stored in the cloud; the cloud server (CS), which is managed by the cloud service provider (CSP) to provide data Storage service and has significant storage space and computation resources; the third party auditor (TPA),who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service reliability on behalf of the user upon request.

Scheme model:



The proposed system specifies that user can access the data on a cloud as if the local one without worrying about the integrity of the data. Hence, TPA is used to check the integrity of data. It supports privacy preserving public auditing. It checks the integrity of the data, storage correctness. It also supports data dynamics & batch auditing.
This paper introduces three entities who are communicating each other for uploading the files into the cloud server. They are

Users:
users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.

Cloud server:
It has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.

Third Party Auditor (TPA):
an optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request. As users no longer possess their data locally, it is of critical importance to assure users that their data are being correctly stored and maintained. In our model, we assume that the point-to-point communication channels between each cloud server and the user is authenticated and reliable, which can be achieved in practice with little overhead.

An auditor understands the service level agreement (SLA) between a customer and a provider and quantities the extent to which a provider might not meet the SLA. The auditor has expertise and capabilities that the customer does not.

Antagonist model:
From user's perspective, the adversary model has to capture all kinds of threats towards his cloud data integrity. There are two kinds of Antagonist models as below.

Weak Adversary: The adversary is interested in corrupting the user's data files stored on individual servers.

Strong Adversary: This is the worst case scenario, in which we assume that the adversary can compromise all the storage servers so that he can intentionally modify the data files as long as they are internally consistent.

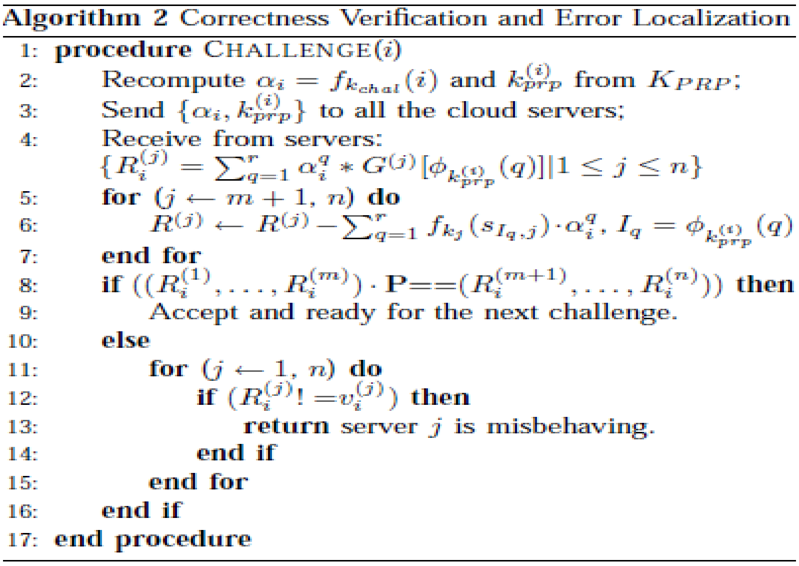
III. SECURITY ANALYSIS

To provide security in this system, the prominent and scalable algorithms are introduced; these are also methods for correctness verification and rectifying errors while uploading the files into the cloud server. The TPA is responsible for performing these algorithms in each abstraction level.

Algorithms used:
Our model introduces some algorithms for verification and error localization.

Algorithm: Accuracy certification And Fault Localization

This algorithm is a key prerequisite for eliminating errors in storage systems. However, many previous schemes do not explicitly consider the problem of data error localization, thus only provide binary results for the storage verification.

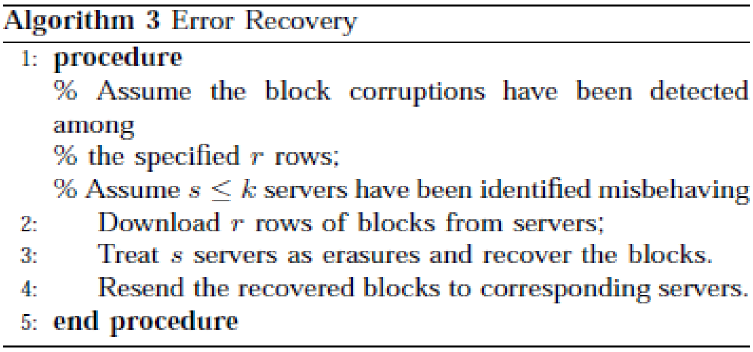


Algorithm 2 Correctness Verification and Error Localization

```
procedure CHALLENGE($i$)
    Recompute $\alpha_i = f_{k_{chal}}(i)$ and $k_{prp}^{(i)}$ from $K_{PRP}$;
    Send $\{\alpha_i, k_{prp}^{(i)}\}$ to all the cloud servers;
    Receive from servers:
    $\{R_i^{(j)} = \sum_{q=1}^{r} \alpha_i^q * G^{(j)}[\phi_{k_{prp}^{(i)}}(q)] | 1 \leq j \leq n\}$
    for ($j \leftarrow m + 1, n$) do
        $R^{(j)} \leftarrow R^{(j)} - \sum_{q=1}^{r} f_{k_j}(s_{I_q,j}) \cdot \alpha_i^q, I_q = \phi_{k_{prp}^{(i)}}(q)$
    end for
    if $((R_i^{(1)}, \ldots, R_i^{(m)}) \cdot \mathbf{P} == (R_i^{(m+1)}, \ldots, R_i^{(n)}))$ then
        Accept and ready for the next challenge.
    else
        for ($j \leftarrow 1, n$) do
            if ($R_i^{(j)} != v_i^{(j)}$) then
                return server $j$ is misbehaving.
            end if
        end for
    end if
end procedure
```

Algorithm: Fault Recapturing

Therefore, the user can always ask servers to send back blocks of the *r* rows specified in the challenge and regenerate the correct blocks by erasure correction, shown in Algorithm, as long as there are at most *k* misbehaving servers are identified. The newly recovered blocks can then be redistributed to the misbehaving servers to maintain the correctness of storage.



Algorithm 3 Error Recovery

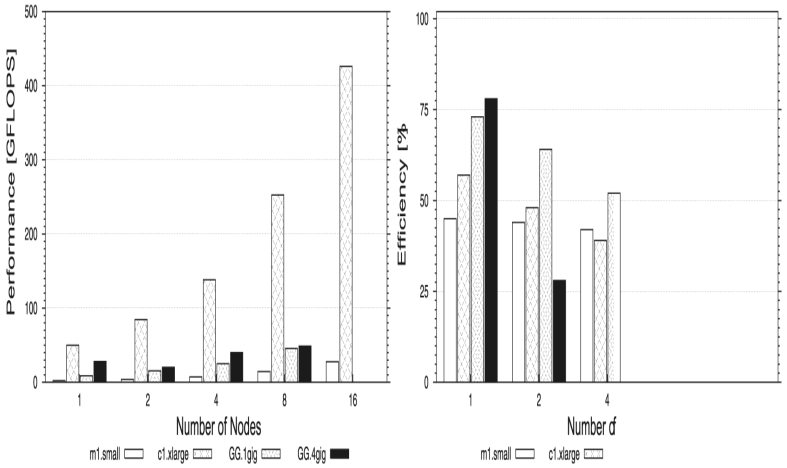
```
procedure
% Assume the block corruptions have been detected among
% the specified $r$ rows;
% Assume $s \leq k$ servers have been identified misbehaving
    Download $r$ rows of blocks from servers;
    Treat $s$ servers as erasures and recover the blocks.
    Resend the recovered blocks to corresponding servers.
end procedure
```

IV. PERFORMANCE ANALYSIS

Cloud computing is an emerging commercial infrastructure paradigm that promises to eliminate the need for maintaining expensive computing facilities by companies and institutes alike. Through the use of virtualization and resource time sharing, clouds serve with a single set of physical resources a large user base with different needs. Thus, clouds have the potential to provide to their owners the benefits of an economy of scale and, at the same time, become an alternative for scientists to clusters, grids, and parallel production environments.

However, the current commercial clouds have been built to support web and small database workloads, which are very different from typical scientific computing workloads. Moreover, the use of virtualization and resource time sharing may introduce significant performance penalties for the demanding scientific computing workloads.

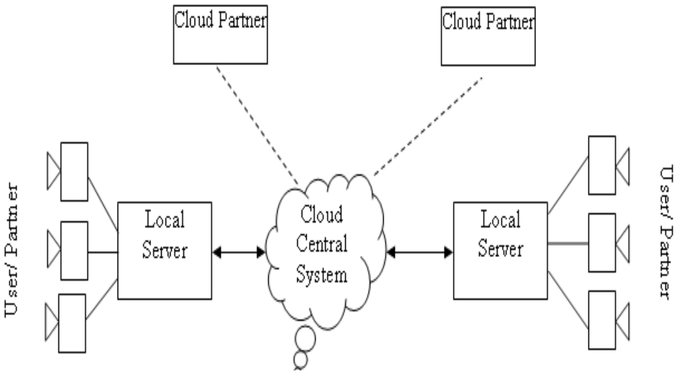
In this work, we analyze the performance of cloud computing services for scientific computing workloads. We quantify the presence in real scientific computing workloads of Many-Task Computing (MTC) users, that is, of users who employ loosely coupled applications comprising many tasks to achieve their scientific goals. Then, we perform an empirical evaluation of the performance of four commercial cloud computing services including Amazon EC2, which is currently the largest commercial cloud. Last, we compare through trace-based simulation the performance characteristics and cost models of clouds and other scientific computing platforms, for general and MTC-based scientific computing workloads. Our results indicate that the current clouds need an order of magnitude in performance improvement to be useful to the scientific community, and show which improvements should be considered first to address this discrepancy between offer and demand.



V. FUTURE SYSTEM OF CLOUD

Recently, technology of cloud computing has been rapidly developed, and it is expected to apply for various network services. Virtual technology is a part of significant technology which has been contributed for the development of cloud computing. Various virtual technologies such as virtual OS and VDE become very important for server and network management in these days. Furthermore, such a virtual technology becomes possible to provide efficient resource management or QoS with virtual network configuration. Thus, it will be important for network construction to provide hardware and software service in near future. Autonomous network configuration in virtual layer is one of such a service. Not only network configuration is constructed in physical layer, but also it should be constructed in virtual layer for providing optimal resource and QoS management. According to our proposed architecture each individual PC act as a cloud partner which offers the necessary resources to the cloud system from its available resources. However each of these individual PC is the property of a particular

Educational institute whereas the institute owned those PCs from the budget sanctioned by the government for that particular institute.



VI. RELATED WORK

The proposed system is an improved framework for POR protocols that generalizes random linear function based holomorphic authenticator. Later it is extended to POR model to distributed systems. This is defined as "provable data possession" (PDP) model for ensuring possession of file on untrusted storages. Their scheme utilized public key based holomorphic tags for auditing the data file, thus providing public verifiability. However, their scheme requires sufficient computation

Overhead that can be expensive for an entire file. This method has lower-overhead than their previous scheme and allows for block updates, deletions and appends to the stored file, which has also been supported in our work. It is not yet clear how the work can be adapted to cloud storage scenario where users no longer have the data at local sites but still need to ensure the storage correctness efficiently in the cloud. The primary improvements are as follows: Firstly, we provide the protocol extension for privacy-preserving third-party auditing, and discuss the application scenarios for cloud storage service. Secondly, we add correctness analysis of proposed storage verification design.

VII. CONCLUSION

This paper, propose a new remote data integrity checking protocol for cloud storage. The proposed protocol supports data insertion, modification and deletion at the block level, and also supports public verifiability. In this paper, we motivate the need for auditing to support an online service-oriented economy. To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users, we propose an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append.

REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," in *Proc. of IWQoS'09*, July 2009, pp. 1–9.

[2] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.

[3] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in *Proc. of SecureComm'08*, 2008, pp. 1–10.

[4] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing,".

[5] Sun Microsystems, Inc., "Building customer trust in cloud computing with transparent security," Online at https://www.sun.