Applied Laser Technology

Vol. 31, No.3, Sep (2024), pp.01-07

Cloud Computing's Transition to Safe and Reliable Storage Services

Mr.Pranav P.Joshi[1], Dr.Sunil Dahale[2], Dr.H.S.Fadewar[3],
Mr.Sunil Nayak[4], Dr.Pawan S. Wasnik [5]
[1]Asst. Prof., Institute of Technology & Management, Nanded, Maharashtra, India
[2]Asst. Prof., MGM College of CS & IT, Nanded, Maharashtra, India
[3]Asst. Prof., School of Computational Science,SRTMU, Nanded, Maharashtra, India
[4]Asst. Prof., Bahirji Smarak Mahavidyalaya Basmat, Hingoli, Maharashtra, India
[5]Asst. Prof., NMDCH, SRTMU Nanded, Maharashtra, India
E-Mail: pranavjoshi13@gmail.com

Abstract:

Cloud storage relieves users of the hassle of managing local hardware and software by allowing them to store their data remotely and take advantage of high-quality cloud applications that are available on demand. Even while these services have many advantages, customers of these services give up physical ownership of their outsourced data, which inherently creates new security issues regarding the accuracy of the data in the cloud. In this work, we offer a flexible distributed storage integrity auditing mechanism, leveraging distributed erasure-coded data and the homomorphism token, to further provide a safe and reliable cloud storage service while addressing this new issue. Users can audit cloud storage with very little computational and connection overhead according to the suggested design. The auditing result accomplishes fast data error localization, or the discovery of misbehaving servers, in addition to providing a robust cloud storage accuracy guarantee.

Keyword: Data Integrity, Dependable distributed storage, error localization, data dynamics and cloud computing.

I. Introduction :

Data centres are becoming massive pools of computing services due to the combination of software as a service (SaaS) computing architecture and ever-cheaper and more powerful CPUs. High-quality services from data and software that only live on remote data centres can now be subscribed to by consumers thanks to growing network bandwidth and dependable but flexible network connections. Users find significant convenience in moving data to the cloud since it relieves them of the hassles associated with direct hardware administration. Two well-known examples of cloud computing pioneers are Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2). Although these internet-based online services offer enormous storage capacity and highly customisable processing capabilities, this shift in computing platforms is also doing away with local workstations' obligation to maintain data. Users must so rely on their cloud service providers to ensure the integrity and availability of their data. On the one hand, a wide range of internal and external threats to data integrity still exist, despite the fact that cloud infrastructures are far more robust and powerful than desktop computers. There are occasionally instances of notable cloud storage service outages and data loss issues. However, since consumers could not keep a local copy of their outsourced data, cloud service providers (CSPs) have different incentives to mislead customers about the state of their outsourced data. For instance, it is feasible for CSP to delete infrequently accessed data without being noticed in a timely manner in order to boost the profit margin by cutting costs. Likewise, CSP might even try to conceal data loss events in order to preserve their good name.

II. **Existing System:**

There were previously a lot of options available for cloud data protection. Here, the methods are dealing with both external and internal threats. It is capable of using higher energy levels. Here, using certain reputation-building strategies offers security resource assurances. It doesn't offer very high security levels. presents the fundamentals of cryptography after a few days. Additionally, it does not provide high performance levels. None of the earlier ones provided satisfactory answers or accurate outcomes in this case. Only static servers are used to disseminate the material to all consumers. Distributing data with a single server is ineffective. Data delivery cannot be assured by a single server. There is no way to get data from another server in the event of a server failure.

Disadvantage

1. Errors may be occurred during input processing

2. Errors in storage

3. There are no error recovery methods available here.

4. This location does not have access to the misbehaviour server.

5. Provide the ambiguous data.

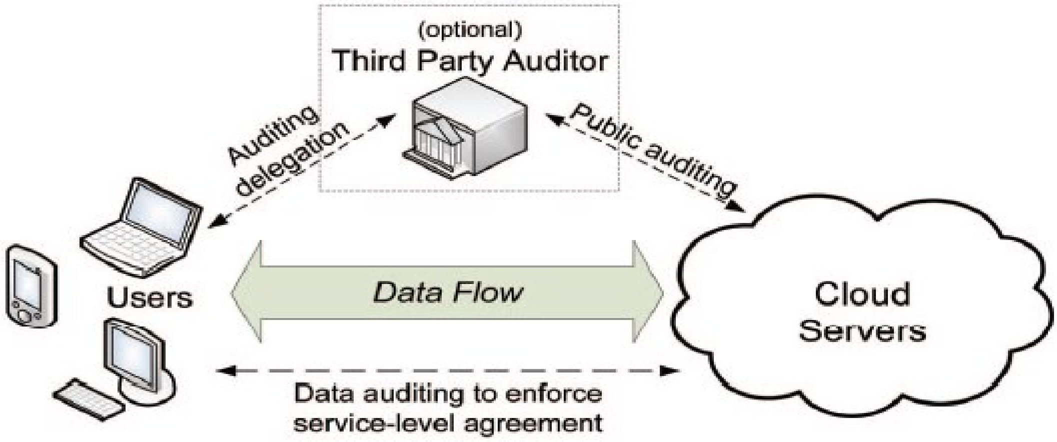
Proposed System:

We are now suggesting the spread of data over multiple servers while implementing distributed protocols. Cross-server storage allows any server to fail while collecting data and distributing high-quality information to users or clients. A data dynamic support technique is what this is known as. It can boost the spread of high-quality data and eliminate issues that are redundant. Data is identified and recovered from replication servers in the event of a server failure. Any issues with data dissemination are displayed by the server, and failed data is recovered from another server. We refer to this as accuracy and verification data.

Advantages:

1. Save the time
2. Save the computation cost.
3. Reduce the burden for users
4. Remove the redundancies

III Architecture:



Software Requirements Specifications:

Software Requirements:

Language	:	java (jdk1.6.0)
Frontend	:	JSP, Servlets
Backend	:	oracle10g
IDE	:	my eclipse 8.6
Operating System	:	windows XP

Hardware requirements:

Processor	:	Pentium IV
Hard Disk	:	80GB
RAM	:	2GB

IV.Modules Description:

1. **System model**
2. **File distribution preparation**
3. **Correctness verification and error localization**
4. **Third party Auditing**
5. **Dynamic data operation support**

System model:

1. **System Model:**
   The network architecture for cloud storage service architecture is illustrated in Fig. 1. Three different network entities can be identified as follows:

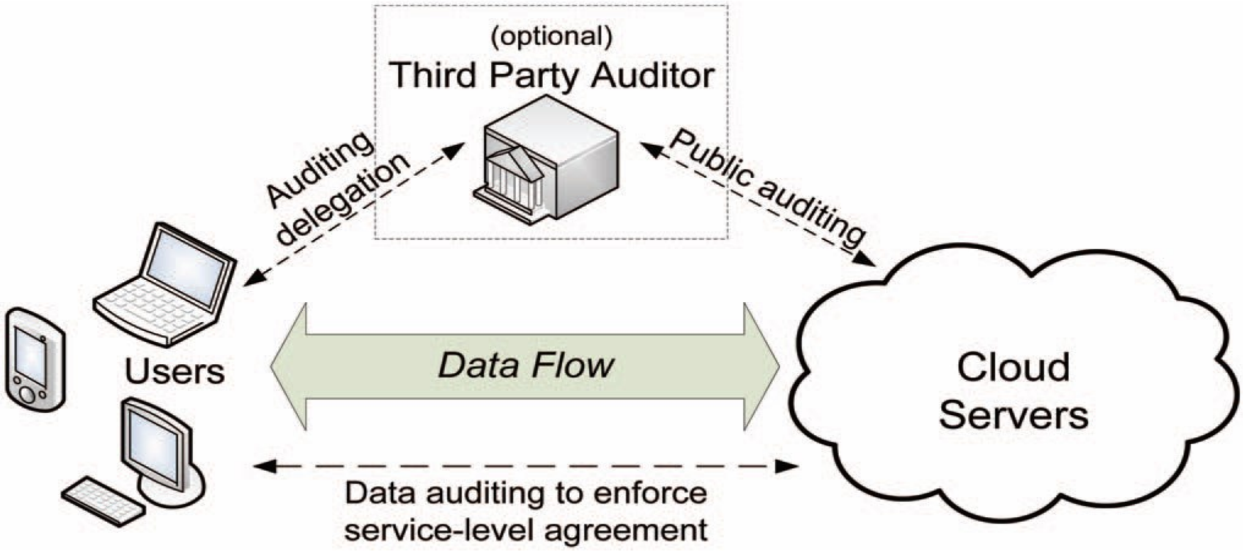


Fig .1 System Model

I. User: An entity might be an enterprise or a single client who needs to store data in the cloud and uses it for compute and data storage.

II. Cloud server (CS) : It is an entity with substantial computational and storage resources that is controlled by a cloud service provider (CSP) to provide data storage services (we will not separate CS and CSP hereafter).

III. Third-Party Auditor: On request, users can rely on an optional TPA with knowledge and skills that they may not have to evaluate and disclose the risk associated with cloud storage services.

2. **File distribution preparation:**
   Primitive Owner (end users/company) Put the information on a cloud server. Backups are maintained by cloud servers, which also maintain replicas (reliable servers). The end user accesses the cloud data to obtain the service whenever he interacts with the owner. Correctness data and end user services fall under the purview of CSP. Each server uses the assistance of another server to accomplish this.

Input: place the Files in cloud server
Process: Security Check and verification
Output: Service providing for end user.

3. **Correctness verification and error localization:**
   A crucial requirement for removing errors from storage systems is error localization. Identifying potential threats from external assaults is also very important. Nevertheless, a lot of earlier techniques merely provide binary findings for the storage verification since they do not specifically address the issue of data error localization. Our scheme performs better than those because we incorporate both error localization (misbehaving server identification) and correctness verification into our challenge-response protocol. Specifically, the response values from servers for each challenge not only identify potential data errors but also determine whether the distributed storage is correct.

Input: Requested files
Process: comparing with correct one's (files).
Output: Identified the misbehaving data.

4. **Third party auditing:**
   As mentioned in our architecture, the user can elect to assign this duty to an impartial third-party auditor, thereby making the cloud storage publicly verifiable, in the event that he lacks the necessary time, resources, or practicality to execute the storage accuracy verification. Nonetheless, no new user data privacy vulnerabilities should be discovered throughout the auditing process in order to safely implement an efficient TPA. In particular, TPA shouldn't discover the content of user data through assigned data auditing. We now demonstrate that our protocol can support privacy-preserving third party auditing with relatively minor modifications.

Input: Requested files and credentials of end user
Process: comparing with correct one's and performs token mechanism.
Output: provide the service to end user by identifying and rectifying the error data.

5. **Dynamic data operation support:** F is thought to stand for static or archival data. Certain application scenarios, like libraries and scientific data sets, can be suitable for this architecture. Nonetheless, there are numerous situations in which data kept in the cloud is dynamic, such as with regard to electronic documents, images, log files, and so forth. Consequently, it is imperative to take into account the dynamic scenario, in which a user may want to alter the data file through a variety of block-level actions, such as appending, deleting, and updating, all while ensuring storage consistency.
   Supporting dynamic data operations might be difficult since data are stored at the address domain of the cloud service provider rather than the local location of the user. CSP must, on the one hand, process the data dynamics request without being aware of

the secret keying information. However, users must confirm that CSP has faithfully handled the complete dynamic data operation request.

Input: Requested files by end users
Process: Updating, adding and deleting.
Output: data modified basing on end user requirement.

V. Conclusion and Future Work

This section outlines our primary plan for guaranteeing cloud data storage in order to solve these issues. The section begins with a review of fundamental coding theory techniques required for our file distribution system among cloud servers. The homomorphism token is then presented. The token computation function under consideration is part of a family of universal hash functions that have been selected to maintain homomorphism features and can be seamlessly used with data verification that has been erasure coded. It is then demonstrated how to derive a challenge-response protocol to both identify misbehaving servers and confirm the accuracy of the storage. Also described is the process for error recovery and file retrieval using erasure-correcting codes. In conclusion, we outline the process of expanding our plan to include third-party audits with minimal changes to the core architecture.

Users of cloud data storage systems no longer own their data locally; instead, it is stored in the cloud. It is necessary to ensure the accuracy and accessibility of the data files being kept on the dispersed cloud servers. Effectively detecting any unauthorised data change and corruption—possibly as a result of server intrusion and/or sporadic Byzantine failures—is one of the most important tasks. Finding the server where the data error is located is crucial in the dispersed situation when such inconsistencies are successfully found, as it can always be the first step towards quickly recovering from storage issues and/or identifying possible external attack risks.

References

[1] Wang.C, Wang.Q, Ren.K, and Lou.W, IEEE INFOCOM, Mar. 2010. [10], "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing" Proc. Wang.C, Ren.K, Lou.W, and Li.J, IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, July/Aug. 2010, "Towards Publicly Auditable Secure Cloud Data Storage Services"

[2] Wang.Q, Wang.C, Li.J, Ren.K, and Lou.W, Proc. 14th European Conf. Research in Computer Security (ESORICS '09), pp. 355- 370, 2009, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing" WANG ET AL.: TOWARD SECURE AND DEPENDABLE STORAGE SERVICES IN CLOUD COMPUTING 231

[3] Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou, IEEE Transactions on Cloud Computing, Volume: 5, Issue: 2, April-June 2012, Towards Secure and Dependable Storage Services in Cloud Computing.

[4] Suresh Arangi & Jayanthi Rao Madina, IJMETMR, http://www.ijmetmr.com/olfebruary2015/SureshArang i-JayanthiRaoMadina-28.pdf, Volume No: 2(2015), Issue No: 2 (February), Flexible and lightweight Storage Auditing Mechanism in Cloud Computing for dynamic operations.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2011, "Towards Secure and Dependable Storage Services in Cloud Computing"

[6] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and S. Chen, IEEE Transactions on Services Computing, accepted, “Dynamic Audit Services for Outsourced Storage in Clouds”

[7] S. Marium, Q. Nazir, A. Ahmed, S. Ahthasham and Aamir M. Mirza, International Journal of Basic and Applied Science, vol 1, no. 3, pp. 177-183, 2012, “Implementation of EAP with RSA for Enhancing The Security of Cloud Computing”

[8] Balkrishnan. S, Saranya. G, Shobana. S and Karthikeyan.S, International Journal of computer science and Technology, vol. 2, no. 2, ISSN 2229-4333 (Print) | ISSN: 0976-8491(Online), June 2012, “Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud”

[9] K. Kiran Kumar, K. Padmaja, P. Radha Krishna, International Journal of Computer science and Technology, vol. 3 pp, ISSN. 0976-8491(Online), pp. 936-940, ISSN: 2229-4333 (Print), March 2012, “Automatic Protocol Blocker for Privacy-Preserving Public Auditing in Cloud Computing”

[10] Jachak K. B., Korde S. K., Ghorpade P. P. and Gagare G. J., Bioinfo Security Informatics, vol. 2, no. 2, pp. 49-52, ISSN. 2249-9423, 12 April 2012, “Homomorphic Authentication with Random Masking Technique Ensuring Privacy & Security in Cloud Computing”

[11] J. Yuan and S. Yu, in Proceedings of ACM ASIACCSSCC’13, 2013, “Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud”

[12] H. Shacham and B. Waters, in the Proceedings of ASIACRYPT 2008. SpringerVerlag,2008,pp.90–107, “Compact Proofs of Retrievability”

[13] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,and D. Song, in the Proceedings of ACM CCS 2007, 2007, pp. 598–610, “Provable Data Possession at Untrusted Stores”