iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** V **Month of publication:** May 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

www.ijraset.com
IC Value: 45.98
Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Secure Data Storage in Cloud

Kiran[1], Shilpa Sharma[2]
[1,2]Department of Computer Science and Engineering
IMS Engineering College, National Highway 24, Near Dasna, Adhyatmik Nagar, Ghaziabad, Uttar Pradesh

Abstract: ***Now-a-days, we have the ability to utilize scalable, distributed computing environments within the confines of the Internet, a practice known as cloud computing. Cloud computing can be said as the long term vision of computing as a utility, where the owners of data can remotely store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources. Due to this, many new security challenges, which have not been well understood. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In this paper, we first design an framework for cloud storage systems and propose an efficient and privacy-preserving auditing protocol. Then, we expand our auditing protocol to support the data dynamic operations, which is efficient and possibly secure in the random oracle model. We expand our auditing protocol to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer. The simulation results show that our proposed auditing protocols are secure and efficient, especially it reduce the computation cost of the auditor. Such an auditing service not only helps save data owners computation resources but also provides a transparent yet cost-effective method for data owners to gain trust in the cloud. We define different approaches and system requirements that should be brought into consideration, and outline challenges that need to be resolved for such a publicly auditable secure cloud storage service to become a reality.***

Keywords: Cloud , Cloud Computing , Data Integrity , Cloud storage techniques, Security techniques, Data Storage.

I. INTRODUCTION

Cloud computing, simply, means internet computing. “Cloud computing” for computation is done through the internet. With cloud computing users can access database resources via the internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources. Besides, databases in cloud are very dynamic and scalable.. The best example of cloud computing is Google apps where any application can be accessed using a browser and it can be deployed on thousands of computer through the internet. It also provides facilities for users to develop, deploy and manage their applications on the cloud, which entails virtualization of resources that maintains and manages itself. Our proposed scheme enables the data owner to delegate tasks of data file re-encryption and user secret key update to cloud servers without disclosing data contents or user access privilege information. We achieve this goal by exploiting and uniquely combining techniques and algorithms (Correctness Verification and Error Localization, traditional replication-based file distribution, adding random perturbations). In this paper, we try to show an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users’ data in the cloud. We are dependent on erasure-correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability. It reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. Cloud computing poses privacy concerns primarily, because the service provider at any point in time, may access the data that is on the cloud. The Cloud service provider could accidentally or deliberately modify or delete some information from the cloud server. Hence, the system must have some sort of mechanism to ensure the data integrity. The current Cloud security model is based on the assumption that the user/customer should trust the provider. This is done by a Service Level Agreement (SLA) that defines mutual provider and user expectations and obligations.

II. RELATED WORK

An effective distributed model with dynamic data support to ensure the correctness of users’ data in the cloud was proposed by C. Wang, Q. Wang, K. Ren, and W. Lou in July 2009. C. Wang, Q. Wang, K. Ren, and W. Lou rely on obliteration correcting code in the file distribution preparation to guarantee the data dependability and redundancies. It reduces the storage overhead as compared to the traditional file distribution techniques. This scheme achieves the storage correctness and data error localization. Whenever data corruption has been detected during the storage correctness verification, this scheme guarantees the localization of data errors. In May 2011, Cong Wang, Qian Wang, Kui Ren, Wenjing Lou extended their work which allows user to audit the cloud storage with very lightweight communication and computation cost. This scheme is highly efficient and resilient against Byzantine failure,

malicious data modification attack and in server colluding attacks.

A formal "Proof of Retrievability" (POR) model was described by A. Juels and J. Burton S. Kaliski in October 2007. It is used for ensuring the remote data integrity. It also combines two methods spot-checking and error- correcting code for ensuring possession and retrievability of files or backup service systems.

It constructed a random linear function based authenticator which highlights unlimited number of queries. It has less communication overhead. The "Provable Data Possession" (PDP) model was defined by Ateniese et al . This model is used for ensuring possession of file on untrusted storages This model uses the public key based homomorphic tags for providing public verifiability. However, this model requires limited computation overhead which may be expensive for an entire file. During 2008, they described a PDP scheme that uses only symmetric key cryptography. This method has lower-overhead than the previous scheme. It provides block updates, deletions and appends on the stored file. However, this model focuses on single server scenario and it does not address small data corruptions, leaving both the distributed scenario and data error recovery issue uncovered. An efficient way of polynomial in the size of the input was proposed by M. A. Shah, R. Swaminathan, and M. Baker during the year 2008 in "Privacy Preserving audit and extraction of digital contents". The main threat from the auditor is that it may glean important information from the auditing process that could compromise the privacy guarantees provided by the service. For example, even a few bits from a file containing medical history could reveal whether a customer has a disease. To ensure privacy, there exist different standards for the encrypted data and the encryption key. For the data, the system relies on (1) the strength of the encryption scheme and (2) the zero-knowledge property of the protocol for encryption-key audits.

To ensure file integrity across multiple distributed servers, using erasure-coding and block-level file integrity checks was proposed by T. S. J. Schwarz and E. L. Miller in 2009. However, their scheme only considers static data files. To verify data integrity using RSA-based hash for data possession in peer-to-peer file sharing networks was defined by D. L. G. Filho and P. S. L. M. Barreto in 2006. However, their proposal requires exponentiation over the entire data file, which is clearly impractical for the server whenever the file is large.

III. PROBLEM STATEMENT

A. *System Model*

1) The network entities can be defined as follows

a) *User:* Users have data which is to be stored in the cloud and rely on the cloud for data computation. It consists of both individual consumers and organizations.

b) *Cloud Service Provider (CSP):* A CSP has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.

c) *Third Party Auditor (TPA):* An optional TPA has expertise and capabilities that users may not have. TPA is trusted to assess and expose risk of cloud storage services on behalf of the users upon request. Implementation of TPA is one of the main goal of this paper .

In this, a user can store his data through a CSP into a set of cloud servers, which are running in a distributed manner. Data redundancy can be employed with technique of erasure-correcting code to further tolerate faults or server crash as user's data grows in size and importance. Therefore, the user interacts with the cloud servers via CSP to access or retrieve his data. 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 case that users do not necessarily have the time, feasibility or resources to monitor their data, they can delegate the tasks to an optional trusted TPA of their respective choices. 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. Note that we don't address the issue of data privacy in this paper, as in Cloud Computing, data privacy is orthogonal to the problem we study here.

B. *Adversary Model*

Security threats that are faced by cloud data storage can come from two different sources. On the one hand, a CSP can be self-interested, untrusted and possibly malicious. It desire to move data that has not been or is rarely accessed to a lower tier of storage than agreed for monetary reasons, but it may also attempt to hide a data loss incident due to management errors, Byzantine failures and so on. On the other hand, there may also exist an economically motivated adversary, who has the capability to compromise a number of cloud data storage servers in different time intervals and subsequently is able to modify or delete user's data while remaining undetected by CSPs for a certain period. We consider two types of adversary with different levels of capability in this

paper: Weak Adversary: The adversary is interested in corrupting the user's data files stored on individual servers. When the server is comprised, an adversary can corrupt the original data files by modifying or introducing its own fraudulent data to prevent the original data from being retrieved by the user. Strong Adversary: This is the worst case scenario, in this we assume that the adversary can compromise all the storage servers so that he can alter the data files since they are internally consistent. In fact, this is where all servers are colluding together to hide a data loss or corruption incident.

C. Design Goals

To ensure the security and dependability for cloud data storage under the aforesaid adversary model, our aim is to design efficient mechanisms for dynamic data verification and operation and achieve the following goals: (1)Correct Storage: to ensure users that their data are stored appropriately and kept untouched all the time in the cloud. (2) Fast localization of data error: to locate the malfunctioning server when data corruption has been easily detected. (3) Dynamic data support: to maintain the level of storage correctness even if users alters their data files in the cloud. (4) Dependability: to enhance data availability against malicious data modification and server colluding attacks or minimizing the effect of data errors or server failures. (5) Minimum Overhead: to enable users to perform correct storage of data with minimum overhead.

IV. SECURITY ANALYSIS AND PERFORMANCE EVALUATION

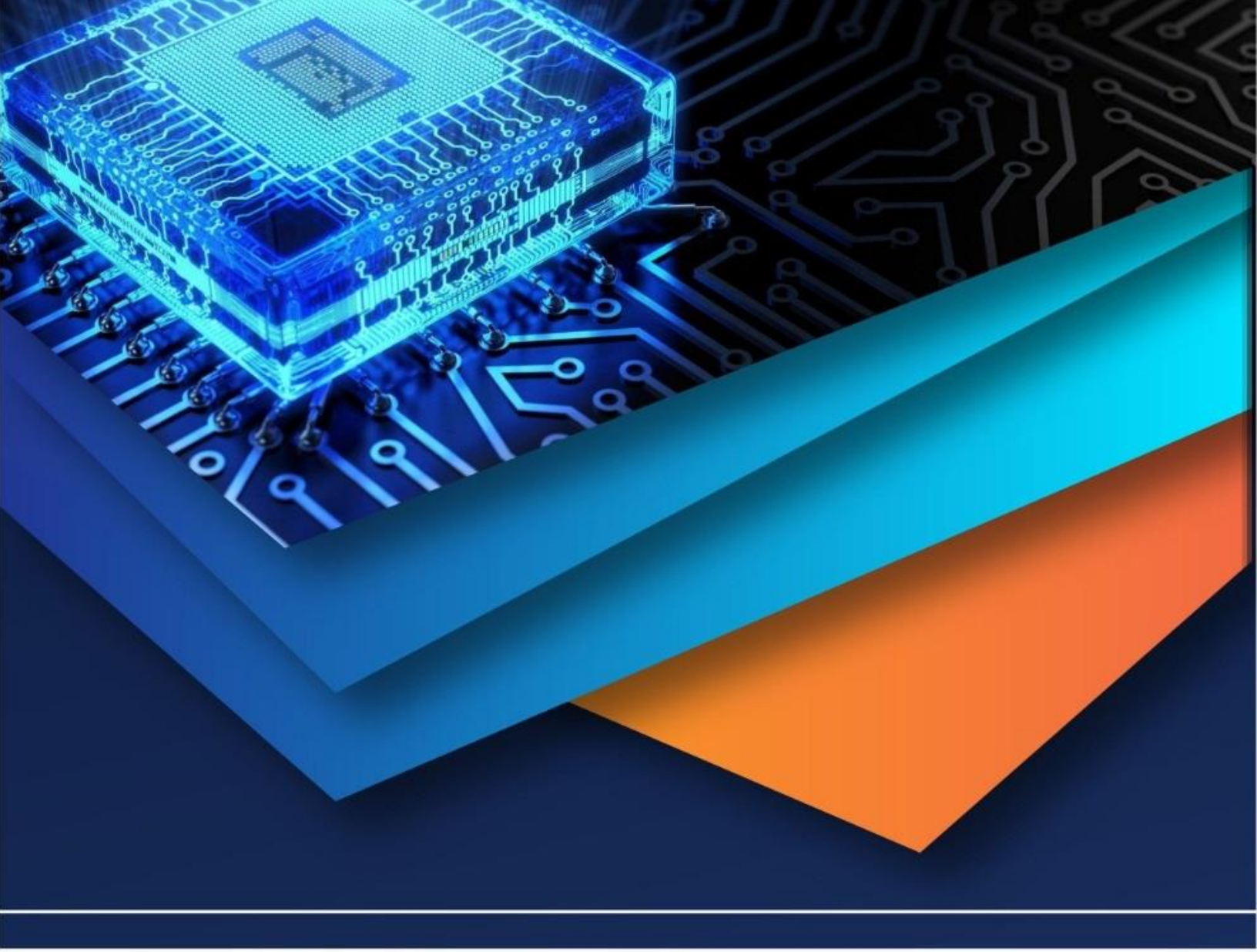
Our security provide an efficiency of our scheme via implementation of both file distribution preparation and verification token pre-computation. In this, servers are required to operate on specified sections to check correctness and verification for the calculation of requested token. We will show that this "sampling" strategy on selected sections can greatly reduce the computational overhead on the server, also maintaining the detection of the data corruption with high probability. Suppose any servers are misbehaving due to the possible compromise or Byzantine failure.

V. CONCLUSIONS

In this paper, we analyse the problem of data security in cloud data storage, which is 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, we propose an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append. We rely on 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 integration of storage correctness insurance and data error localization, i.e., whenever data corruption has been detected during the storage correctness verification across the distributed servers, we can almost guarantee the simultaneous identification of the misbehaving server(s). Considering 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 depute the integrity checking tasks to third-party auditors and be worry-free to use the cloud storage services. By providing detailed security and extensive experiment results, we show that our scheme is highly efficient and resilient to Byzantine failure, malicious data modification attack.

REFERENCES

[1] YunchuanSun, JunshengZhang, YongpingXiong, and GuangyuZhu, "Data Security and Privacy in Cloud Computing" in Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2014, Article ID 190903, 9 pages http://dx.doi.org/10.1155/2014/190903
[2] Aizah Amin Soofi , M.Irfan Khan, "A Review Paper On Data Security in Cloud"
[3] Manpreet Kaur, Hardeep Singh, "A Review of cloud computing security issues" in International Journal of Advances in Engineering & Technology, June, 2015
[4] Jagjit Singh, Er. Gurjit Singh Bathal, "A Review on Storage Security Challenges in Cloud Computing" in Volume 5, Issue 6, June 2015 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering
[5] Karun Handa et al, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, May- 2015, pg. 786-791
[6] Balasubramanian V.1 and Mala T.,"A Review on various data security issues in cloud computing environment and its solutions" in VOL.10,NO. 2, FEBRUARY2015 ISSN 1819-6608 ARPN Journal of Engineering and Applied Sciences



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY