www.ijecs.in
*International Journal Of Engineering And Computer Science ISSN: 2319-7242*
*Volume 4 Issue 12 Dec 2015, Page No. 15107-15110*

# STUDY ON ENSURING DATA STORAGE SECURITY SYSTEM IN CLOUD COMPUTING SERVICE

**K..Kavitha**
Assistant Professor, Department of Computer Applications
Adhiparsakthi Engineering College
Email: kavithaapec@gmail.com

## Abstract:

*Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trust worthy. This unique paradigm brings about many new security challenges, which have not been well understood. This paper proposed a problem of ensuring the integrity of data storage in Cloud Computing. In particular, consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. While prior works on ensuring remote data integrity often lacks the support of either public auditability or dynamic data operations, first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works.*

**Keywords :** Data storage, public auditability, data dynamics, cloud computing, Protocol.

## 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 hugeIn Cloud Computing, the remotely stored electronic data might not only be accessed but also updated by the clients, e.g., through block modification, deletion, insertion, etc. Unfortunately, the state of the art in the context of remote data storage mainly focus on static data files and the importance of this dynamic data updates has received limited attention so far Moreover, as will be shown later, the direct extension of the current provable data possession (PDP) or proof of irretrievability (POR) schemes to support data dynamics may lead to security loopholes. Although there are many difficulties faced by researchers, it is well believed that supporting dynamic data operation can be of vital importance to the practical application of storage out sourcing services. In view of the key role of public audit ability and data dynamics for cloud data storage, proposed an efficient construction for the seamless integration of these two components in the protocol design motivate the public auditing system of data storage security in Cloud Computing, and propose a protocol supporting for fully dynamic data operations, especially to support block insertion, which is missing in most existing schemes. Extending the scheme to support scalable and efficient public auditing in Cloud Computing.[2]

## II. SYSTEM MODEL

Representative network architecture for cloud data storage. Three different network entities can be identified as follows:

• **User:** 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[7].

• **Cloud Service Provider (CSP):** a CSP, who 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. In cloud data storage, a user stores his data

Laboratory's /16 networks.We deployed Honeyd responders on five of the subnets and operated the other five completely "dark.[6]"

## III. ADVERSARY MODEL

Security threats faced by cloud data storage can come from two different sources. On the one hand, a CSP can be self-interested, entrusted and possibly malicious. Not only does 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.[4]

Adversary, who has the capability to compromisea number of cloud data storage servers in different time intervals and subsequently is able to modify or delete users' data while remaining undetected by CSPs for a certain period.

**Weak Adversary:** The adversary is interested in corrupting the user's data files stored on individual servers. Once a server is comprised, an adversary can pollute 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 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. In fact, this is equivalent to the case where all servers are colluding together to hide a data loss or corruption incident.

## IV. SYSTEM ARCHITECTURE

To ensure the security and dependability for cloud data storage under the aforementioned adversary model, to design efficient mechanisms for dynamic data verification and operation and achieve the following goals[9]

(1) **Storage correctness** to ensure users that their data are indeed stored appropriately and kept intact all the time in the cloud.

(2) **Fast localization** of data error: to effectively locate the malfunctioning server when data corruption has been detected.

(3) **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.

(4) **Dependability** 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.

(5) **Lightweight** to enable users to perform storage correctness checks with minimum overhead.Monotonically scanning the destination IP addresses (e.g., sequentially one after another) is a scan strategy widely used by network scanning tools. For random events, the monotonic trend checking can help filter out the noises caused by the non-bot scanners.

## V.ENSURING CLOUD DATA STORAGE

In cloud data storage system, users store their data in the cloud and no longer possess the data locally. Thus, the correctness and availability of the data files being stored on the distributed cloud servers must be guaranteed. One of the key issues is to effectively detect any unauthorized data modification and corruption, possibly due to server compromise and random Byzantine failures. Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance, since it can be the first step to fast recover the storage errors.

To address these problems, our main scheme for ensuring cloud data storage is presented in this section. The first part of the section is devoted to a review of basic tools from coding theory that are needed in our scheme for file distribution across cloud servers.

DOI: 10.18535/Ijecs/v4i11.40

## VI. PROVIDING DYNAMIC DATA OPERATIONSUPPORT

This model may fit some application scenarios, such as libraries and scientific datasets. However, in cloud data storage, there are many potential scenarios where data stored in the cloud is dynamic, like electronic documents, photos, or log files etc. Therefore, it is crucial to consider the dynamic case, where a user may wish to perform various block-level.[12]

Operations of update delete and append to modify the data file while maintaining the storage correctness assurance. The straightforward and trivial way to support these operations is for user to download all the data from the cloud servers And re-compute the whole parity blocks as well as verification tokens. This would clearly be highly inefficient. In this section, we will show how our scheme can explicitly and efficiently handle dynamic data operations for cloud data storage.

## VII.CONCLUSION

Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about 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 particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud is indeed intact. The support for data dynamics via the most general forms of data operation, such as block modification, insertion and deletion, is also a significant step toward. Another major concern is how to construct verification protocols that can accommodate dynamic data files. In this technology, explored the problem of providing simultaneous public audit ability and data dynamics for remote data integrity check in Cloud Computing.

## REFERENCES


1. T. Schwarz and E.L. Miller, (2006), “Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage,”Proc. 26th IEEE Int’l Conf. Distributed Computing Systems (ICDCS’06).
2. K.D. Bowers, A. Jules, and A. Opera, (2008), “Proofs of Irretrievability: Theory and Implementation,” Report 2008/175, Cryptology print Archive.
3. K.D. Bowers, A. Juels, and A. Oprea, (2009), “Hail: A High-Availability and Integrity Layer for Cloud Storage,” Proc. 16th ACM Conf. Computer and Comm. Security.
4. Q. Wang, K. Ren, W. Lou, and Y. Zhang, (2009), “Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance,” Proc. IEEE INFOCOM, pp. 954-962.
5. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, (2009), “Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing,” Proc. 14th European Symp.Research in Computer Security (ESORICS ’09).
6. M. Naor, G.N. Rothblum,“The Complexity of Online Memory Checking”, Proc. 46th Ann. IEEE Symp. Foundations of Computer Science (FOCS ’05), pp. 573-584, 2005.
7. E.-C. Chang, J. Xu,“Remote Integrity Check with Dishonest Storage Server”, Proc. 13th European Symp. Research in Computer Security (ESORICS ’08), pp. 223-237, 2008
8. M.A. Shah, R. Swaminathan, M. Baker,“Privacy-Preserving Audit and Extraction of Digital Contents”, Report 2008/186, Cryptology ePrint Archive, 2008.
9. A. Oprea, M.K. Reiter, K. Yang,“Space-Efficient Block Storage Integrity,” Proc. 12th Ann. Network and Distributed System Security Symp. (NDSS ’05), 2005.
10. T. Schwarz and E.L. Miller,“Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage”, Proc. 26th IEEE Int’l Conf. Distributed Computing Systems (ICDCS’06), p. 12, 2006.
11. Q. Wang, K. Ren, W. Lou, Y. Zhang,“Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance”, Proc. IEEE INFOCOM, pp. 954-962, Apr. 2009.
12. G. Ateniese, R.D. Pietro, L.V. Mancini, G. Tsudik, “Scalable and Efficient Provable Data Possession”, Proc. Fourth Int’l Conf. Security and Privacy in

Comm. Networks (SecureComm '08), pp. 1-10,2008.

13. C. Wang, Q. Wang, K. Ren, and W. Lou,"Ensuring Data Storage Security in Cloud Computing", Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), 2009.
14. C. Erway,A. Kupcu, C. Papamanthou, R. Tamassia, "Dynamic Provable Data Possession", Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), 2009.
15. K.D. Bowers, A. Juels, A. Oprea,"Hail: A High-Availability and Integrity Layer for Cloud Storage", Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 187- 198, 2009.
16. D. Boneh, B. Lynn, H. Shacham,"Short Signatures from the Weil Pairing", Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '01), pp. 514-532, 2001. [18] R.C. Merkle, "Protocols for Public Key Cryptosystems", Proc.