**Data Integrity and Dynamic Storage Way in Cloud Computing**

**ABSTRACT**

It is not an easy task to securely maintain all essential data where it has the need in many applications for clients in cloud. To maintain our data in cloud, it may not be fully trustworthy because client doesn’t have copy of all stored data. But any authors don’t tell us data integrity through its user and CSP level by comparison before and after the data update in cloud. So we have to establish new proposed system for this using our data reading protocol algorithm to check the integrity of data before and after the data insertion in cloud. Here the security of data before and after is checked by client with the help of CSP using our ―effective automatic data reading protocol from user as well as cloud level into the cloud‖ with truthfulness. Also we have proposed the multi-server data comparison algorithm with the calculation of overall data in each update before its outsourced level for server restore access point for future data recovery from cloud data server. Our proposed scheme efficiently checks integrity in efficient manner so that data integrity as well as security can be maintained in all cases by considering drawbacks of existing methods

**EXISTING SYSTEM**

The traditional cryptographic technologies for data integrity and availability, based on Hash functions and signature schemes cannot work on the outsourced data. it is not a practical solution for data validation by downloading them due to the expensive communications, especially for large size files. Moreover, the ability to audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users. Therefore, it is crucial to realize public audit ability for CSS, so that data owners may resort to a third party auditor, who has expertise and capabilities that a common user does not have, for periodically auditing the outsourced data. This audit service is significantly important for digital forensics and credibility in clouds. To implement public audit ability, the notions of proof of retrievability and provable data possession have been proposed by some researchers. Their approach was based on a probabilistic proof technique for a storage provider to prove that clients’ data remain intact.

**Disadvantages:**

* Lack of rigorous performance analysis for constructed audit system greatly affects the practical application of this scheme.
* it is crucial to develop a more efficient and secure mechanism for dynamic audit services, in which possible adversary’s advantage through dynamic data operations should be prohibited
* Single TPA to audit for all files and to take more time to auditing the files.

**PROPOSED SYSTEM**

In this paper, we introduce a dynamic audit service for integrity verification of untrusted and outsourced storages. Our audit system, based on novel audit system architecture, can support dynamic data operations and timely abnormal detection with the help of several effective techniques, such as fragment structure, random sampling, and index-hash table. Furthermore, we propose an efficient approach based on probabilistic query and periodic verification for improving the performance of audit services. A proof of- concept prototype is also implemented to evaluate the feasibility and viability of our proposed approaches. Our experimental results not only validate the effectiveness of our approaches, but also show our system has a lower computation cost, as well as a shorter extra storage for integrity verification

**Advantages:**

* A fragment technique is introduced in this paper to improve performance and reduce extra storage.
* The audit activities are efficiently scheduled in an audit period, and a TPA needs merely access file to perform audit in each activity.
* Each TPA to audit for a batch of files and to save the times for auditing the files.

**MODULE DESCRIPTION:**

1. **Cloud User:** the user, who can be an individual or an organization originally storing their

data in cloud and accessing the data.

1. **Cloud Service Provider (CSP):** the CSP, who manages cloud servers (CSs) and

provides a paid storage space on its infrastructure to users as a service.

1. **Third Party Auditor (TPA) or Verifier:** the TPA or Verifier, who has expertise and

capabilities that users may not have and verifies the integrity of outsourced data in cloud

on behalf of users. Based on the audit result, the TPA could release an audit report to

user.

**System Requirement:**

**Hardware Requirements**

* System : Pentium IV 2.4 GHz
* Hard disk : 40 GB
* Monitor : 15 VGA colour
* Mouse : Logitech.
* Ram : 256 MB
* Keyboard : 110 keys enhanced.

**Software Requirements**

* **Operating System :** Windows
* **Programming language:** c#.Net
* **Web-Technology:** ASP
* **Front-End:** ASP.NET
* **Back-End:** SQL SERVER