**LITERATURE SURVEY**

**1) Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing.**

**AUTHORS:** C. Wang, Q. Wang, K. Ren, and W. Lou,

Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homomorphism authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

**2) Data dynamics for remote data possession checking in cloud storage**

**AUTHORS :-** Lanxiang Chen, Shuming Zhou, Xinyi Huang, Li Xu.

In cloud storage, storage servers may not be fully trustworthy. Therefore, it is of great importance for users to check whether the data is kept intact. This is the goal of remote data possession checking (RDPC) schemes. In this paper, an RDPC scheme based on homomorphism hashing is proposed. To enable data dynamics, the Merkle hash tree is introduced to record the location for each data operation in the scheme. Data dynamics, including the most general forms of data operations such as block modification, insertion and deletion, are supported. Our scheme provides provable data possession and integrity protection. The security and performance analysis shows that the scheme is practical for real-world use.

**3)**  **Efficient public verification on the integrity of multi-owner data in the cloud.**

**AUTHORS :-**  B.Wang, H. Li, X. Liu, F. Li, and X. Li.

Cloud computing enables users to easily store their data and simply share data with others. Due to the security threats in an un-trusted cloud, users are recommended to compute verification metadata, such as signatures, on their data to protect the integrity. Many mechanisms have been proposed to allow a public verifier to efficiently audit cloud data integrity without receiving the entire data from the cloud. However, to the best of our knowledge, none of them has considered about the efficiency of public verification on multi-owner data, where each block in data is signed by multiple owners. In this paper, we propose a novel public verification mechanism to audit the integrity of multi-owner data in an un-trusted cloud by taking the advantage of multi-signature s. With our mechanism, the verification time and storage overhead of signatures on multi-owner data in the cloud are independent with the number of owners. In addition, we demonstrate the security of our scheme with rigorous proofs. Compared to the straightforward extension of previous mechanisms, our mechanism shows a better performance in experiments.