Different blocks in shared data are generally signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks which were previously signed by this revoked user must be re-signed by an existing user.

B. Boyang Wang,et.al.(2014), Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud;

In this paper, They propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular, they exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With those mechanisms, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, those mechanisms are able to perform multiple auditing tasks simultaneously instead of verifying them one by one and experimental results demonstrate the effectiveness and efficiency of those mechanisms when auditing shared data integrity.

C. CongWang,et.al.(2013),Privacy-Preserving Public Auditing for Secure Cloud Storage;

Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public audit ability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. In this paper, they propose a secure cloud storage system supporting privacy-preserving public auditing. They further extend those result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. Those preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design.

D. M. Armbrust,et.al.(2010),A View of Cloud Computing, Communications of the ACM;

cloud computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about over provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under provisioning for one that becomes wildly popular, thus missing potential customers and revenue.

E. C.Wang,et.al.(2010),Privacy-Preserving Public Auditingfor Data Storage Security in Cloud Computing

Cloud Computing has been envisioned as the nextg eneration architecture of IT Enterprise. It moves the application software and databases to the centralized large data centres, 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, they 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 client through the auditing of whether his data stored in the cloud is indeed intact, which can be important in achieving economies of scale for Cloud Computing. The support for data dynamic svia the most general forms of data operation, such as block modification, insertion and deletion, is also a significant step toward practicality, since services in Cloud Computing are not limited to archive or backup data only. While prior works on ensuring remote data integrity often lacks the support of either public verifiability or dynamic data operations, this paper achieves both. They first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for seamless integration of these two salient features in those protocol designs. In particular, to achieve efficient data dynamics, they improve the Proof of Retrievability model by manipulating the classic Merkle Hash Tree (MHT) construction for block tag authentication Extensive security and performance analysis show that the proposed scheme is highly efficient and provably secure.

F. G. Ateniese,et,al.(2007),Provable Data Possession at Untrusted Stores, in the Proceedings of ACM CCS 2007

they introduce a model for provable data possession (PDP)that allows a client that has stored data at an un trusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage systems.

3. Proposed System

Our proposed system avoid losing money on data sharing services it may lie to examiners about the false shared data for saving the reputation of its data services. Here we consider an assumption to avoid collusion between user and the cloud.