**LITERATURE SURVEY**

Bhavna Makhija et.al, presented a study related to the various data security and privacy techniques applied in cloud applications. Issues such as lack in integrity of data, lack of support for dynamic data operations, and lack of availability of high resource and computation cost were identified in different techniques. Further, the TPA was applied in order to provide a clear view of all the data security techniques and methods which previously exist [7]. Higher efficiency can be provided by applying the private audit ability. However, the ability of challenging the cloud server to ensure correctness of data storage is provided through public audit ability.

Dawn Song et.al, presented that the per-application development effort using which the data can be protected is minimized by the proposed architecture called DPaaS [8]. For balancing the huge development and easy maintenance along with the verification of user-side, the key management and access control process are moved to the middle tier known as computing platform. The privacy at the required granularity is not the concern of FDE even though the performance and ease of development are provided by it. However, the data visibility is removed completely from both server and application developer by the FHE.

Deyan Chen et.al, provided a study related to the various issues being faced by the data when it crosses the data life cycle in terms of maintaining its security and privacy [9]. The future research of the data security and privacy protection problems being faced in cloud is also presented here. There is still the need to solve various problems of cloud computing even though it provides several benefits. There is a revenue estimation conducted for cloud computing which shows that its demand is increasing with the passage of time. The threats from hackers are increasing however, due to the presence of existing vulnerabilities within the cloud model.

Deepan chakaravarthi et.al, proposed a distributed approach through which the data stored in clouds can be secured. It is ensured here that the unauthorized access of data is not performed here. The homomorphism token is applied along with distributed verification of the erased coded data to provide security [10]. The data is stored, recognized at the cloud server and few of its tasks are executed by applying the proposed technique. This paper also ensures the collision attacks are avoided such that the unauthorized users do not make modifications on the server. The various problems being faced on the security of data within cloud data storage are studied here so that proper measures can be taken.