**Introduction**

A scenario in which the resources can be accessed from a shared pool as per the demand and convenience of user is known as cloud computing. The management required for these resources is very less. There are several clients and organizations which store their private data within the clouds. This data can be modified or retrieved by the users as per their requirements. The “pay per user” method is used here in order to provide services to the cloud users. This means that the users only need to pay for the services they access for a certain period of time. Cloud computing is basically a technology through which the wide range of applications can be accessed by users that have different topologies. The specialization for each topology is different. It is possible to have access to any user’s account without its knowledge through the cloud service providers provided in this technology. However, huge data might be lost here which cannot be handled by the user. Several security problems are being faced within cloud computing and depending upon certain criterions these problems can be categorized. In order to provide security to the information available within clouds, different types of data security approaches have been developed over the years by researchers. The researchers have been discussing over the best possible solutions to be provided within certain scenarios.

**1.1 Overview of Project**

The encryption technique in which the corresponding algebraic function is used to handle plain and cipher texts is known as homomorphic encryption. The algebraic operation which is applied on both of these texts is connected even when the texts are not connected. The technique through which the data is encrypted in such a manner that a query- specific token is used for querying it is known as structured encryption. The knowledge from secret key is used in order to generate this query-specific token.

Also, the information related to query or data is not revealed by the query process. Therefore, the major concern here is the representation of ‘f’ function which can be different for various schemes. There are, several security and maintenance related challenges being faced by the technologies today which cannot be resolved by applying the FDE and FHE. This can be understood more clearly by highlighting the differences that exist amongst them such as:

**Key management and trust**: The keys might be available within the cloud platform or near to the physical drive in case of FDE. The key management process does not include the cloud application user. Even though the data of user is encrypted on the physical disk, any layer present below it can access it at any time. Thus, the access of data to unauthorized users of online attacks is not prevented by FDE approach. The data cannot be learnt or leaked easily .Through the untrusted applications when FHE is applied. The FHE encryption keys are owned and managed by the users. However, without seeing the data actually, computations can be performed on encrypted forms by the applications.

**1.2 Motivation**

For the cloud applications, another important feature to be considered is collaboration. To make it possible for the owner to share one or more data objects selectively with other users, it is important to include fine- grained access control. Since the access control granularity and key granularity are not lined up, it is important for a user to completely rely on the cloud provider for providing the right access control in the presence of FDE. There is no exact way defined for providing access control yet, since the encryption keys are managed by the user or third party cloud provider in case of FHE. The key management can be defined on a per- data object granularity basis such that the fine-grained encryption-based access control can be provided. It is important for the objects to be encrypted with in similar public key for supporting homomorphic operations within the multiple encrypted objects.

**Performance**: The symmetric encryption of FDE can be performed at the complete bandwidth of disk due to which the system slows down its processing. Before being capable enough to deploy at a scale, it is important to enhance the performance of FHE.

**Ease of development**: There is no impact of FDE on the development of application since it is hidden behind an abstraction of physical disk. There might be the possibility of relative automaticity for FHE which states that on an abstraction of program FHE works as a circuit which is then transformed.

**Maintenance**: It is impossible to prevent a system from all the errors or bugs. The most important goal of clouds is availability due to which it is important to ensure that the systems are debugged. There is a need for an individual to step in and manually check the reasons when a system failure occurs randomly. There is a need to detect an unusual activity or understand the actual problem in order to determine the nature of problem. In case of FHE, this however, might be difficult. It would be difficult to perform debugging if the application writer cannot inspect the application state in a meaningful manner.

**1.3 Problem Definition**

The problems related to the security of cloud computing. The cloud computing security is separated from other computing security techniques since the data shared with CSP is recognized as core scientific issue. In order to protect the data from cloud infrastructure provider different techniques have been utilized by researchers. Further, the FHE techniques are applied within the cloud applications to highlight the few difficulties. A technique through which the SAAS. 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. The data is stored, recognized at the cloud server and few of its tasks are executed by applying the technique to get the data.

**1.4 Objectives of Project**

Project objectives are specific and are considered lower-level statements. We can describe the results, specific, tangible deliverables that the project will produce at the run time. Progress towards an objective can usually be tracked with a project dashboard because objectives are often associated with metrics. Objectives are stated clearly as they are going to influence every decision in the project throughout its life cycle. Like project goals, objectives must be measurable as they will decide whether a project is a success or not. Therefore, objectives contain such as budget, quality and how long it takes to finish the project code and what are the software using to host it.

**1.5 Limitations of Project**

On their other hand project management also has some drawbacks and limitations which one should seriously comfier. These limitations are listed below:

The project plan can’t be complicated; it needs a certain degree of simplification. Project management may leads to a complex project plan which sometimes is misleading to those working on the project, and if you don’t understand the project plan, then it becomes very difficult to deliver what is expected from you.

Changes to the project planning diagram may require more replanting time that can be tolerated. The project planning diagram should be very flexible and open to the changes and modifications.