CHAPTER 7

CONCLUSION AND FUTURE ENHANCEMENT

7.1 CONCLUSION

The cloud computing environment provides an effective storage mechanism for the organizations due to their enormous advantages. This technology has adopted by several organizations but not in a broad manner due to the security and confidentiality issues it faces. The information is stored in the cloud storage which is totally under the influence of service providers. These service providers serve the users as per their demand and it must not allow any malicious users to gain access to the stored information.

Since it is known that the users require only that information that they use for performing a particular set of tasks. It is necessary to safeguard other information from the users who try to gain access due to their malicious behavior for which the users are cataloged based on the request they make for acquiring information for performing the task and also by verifying their identity so that the service provider very well can identify the users requested for information and it serves accordingly. The scheme retards the malicious activities into the system since the access mechanism happens in a safe and secure manner using some sort of secret keys. After verifying the user identity the information is passed on to the users from the service provider by encrypting the information using cryptographic methods which shares keys.
between the users and the service providers through an authorizer which verifies that the key is held by privileged users.

The portrayal is with the insight of user segregation based on the queries i.e. the requirements of the users which have to be served by the suppliers of the cloud. For minimizing the security problems the users are segregated based on their queries based on which they will be served. The fetching of queries varies in terms of associations with the concept and fetched data. It is to be noted that all these process are achieved based on the semantics i.e. input from the user.

The focus is on providing safety while verifying the user requirements after obtaining the queries of the users based on which the requirements will be analyzed by the message inspector. The requirements are matched to the user queries to verify the trueness in offering the required requests. The message inspector performs the task of verifying the trueness of the acquired data based on the results fetched based on the user queries and are analyzed in terms of accuracy, occurrence and indexing.

The cloud computing as detailed in the previous chapters offers several services to the users based on their requirements. The users of the cloud make use of these services through the internet. Since the services are offered through the internet it is necessary to focus on the safety and confidentiality of the information offered to the users by the cloud service providers. There is a chance that the attackers might gain access to the information while it is being transferred to the intended users. The scheme provides a clear insight for safeguarding the information while it is being transferred to the users. The allowed users can only be able to gain access to the information.
The proposed scheme offers a better way for communication between the service providers and the consumers without compromising the security and confidentiality of the stored information. The technique outperforms the other conventional mechanisms and attains good performance in cloud computing environment.

It is already discussed that the queries must match the concepts for acquiring the expected results. The user segregation scheme attempts to segregate the users based on the requirements which is inspected and verified by message inspector. The security aspects are performed on the query before delivering it to the users. It is evident that the scheme acquires 79% of efficiency as compared to the conventional homomorphic based encryption schemes.

7.2 FUTURE ENHANCEMENT

The work can be further elaborated by designing a hybrid security scheme for offering safety and confidentiality for the services offered by the cloud computing at the service provider levels in addition to the third party investigation.