CHAPTER 8

CONCLUSION AND FUTURE ENHANCEMENTS

8.1. CONCLUSION

The instant communication channel key organizer model is presented for providing secure sharing of data in cloud environment. The creation of an instant communication channel assigned with a specific id for the cloud users provides an efficient communication security in cloud. The data requested by users are sent by the cloud service provider to the Belief Inspector who verifies the authorization of data in an effective manner. The data access is provided only to the authorized users and thus the malicious users are prevented from usage of data by means of Belief Inspector. Hence, the leakage of data to unauthorized users is reduced in a significant manner.

Moreover, the conditional source trust attribute encryption with particle swarm based transaction optimization framework is proposed for ensured transactional security of data in cloud servers. The security level of data transactions on cloud storage has increased by applying conditional source trust attribute based encryption and decryption method along with a cipher specific id number. Multiple delegated tasks from users are effectively handled by means of bilinear mapping process. The particle swarm based transaction optimization technique helps in providing best result of data transaction from the entire population of information in cloud using the fitness function to cloud users. Hence the transaction completion time of cloud applications is minimized.

In addition to this, the data storage capacity is improved and the consistency of data during concurrent transactions is maintained efficiently by applying the linear erasure correction model. The throughput level of data transactions are increased by assigning multi-threaded state transition mechanism. Based on the on-demand transaction request of users, the storage states and threads are assigned by the
Poisson exponential distribution method thus producing increased cyclic progression ratio.

Hence the novel secure cloud data storage mechanism provides ensured communication and transaction security for the concurrent cloud applications. Moreover, the performance of the novel secure cloud data storage mechanism based on ICCKO, CSTAE-PSTO and LE-PED framework was found to be efficient when compared to the other existing methods.

8.2. FUTURE ENHANCEMENTS

The instant communication channel key organizer model is introduced to identify the leakage of data and improve the leakage detection rate with the help of belief inspector. This in turn reduces the probability of data leakage in the system. However, the organization key model may require larger key size. Due to this, it affects the resource utilization of the system and results in improved computation complexity. The further work can be preceded with an effective encryption and decryption key model with smaller key size.

In addition to this, the cloud data security level is increased in a significant manner using the conditional source trust attribute encryption method along with unique cipher specific identity number. The optimization of specific id is performed using particle swarm based transaction optimization method for reducing the transaction completion time. However, the cloud services provides higher computation cost of data transaction. Hence, the further work can be implemented with minimum cost of transaction of data on cloud servers.

Next, in order to enhance the cloud data storage capacity and data consistency, the linear erasure correction model is applied for several user transactions. However, the file replication is a challenging issue in cloud data transactions. The further work can be preceded with cloud storage security technique to improve the security with minimum computation time. This technique needs to be address the file replication strategy for maintaining the higher consistency level. It is also used to reduce the consistency overhead by means of maintaining number of replicas on cloud servers. This can help to improve the secure sharing of data to cloud users.