CHAPTER 6

CONCLUSIONS AND SCOPE FOR FURTHER STUDY

6.1 Conclusions

In this thesis, the main objective is to make the data secure in the cloud. To achieve that data security contrivance was implemented and experimented to protect data. The other objective is prevention of unauthorized access, more throughput, and securing data from hackers. Most of the cryptographic algorithm spends more time in processing the data. A simple and easy to implement modified blowfish algorithm has been proposed which has reduced the processing time whenever the data is sent from client side. This algorithm can be easily implemented and embedded with existing algorithm. To reduce the transmission time and safe retrieval of data from the cloud storage server, an enhanced social spider optimization algorithm is proposed along with signcryption algorithm. In this data is embedded in image by finding blue pixel. This minimizes the chance of data going to hackers since it is hard to find data in pixel.

Enhanced optimization algorithm also ensures retrieval of data in safe manner at the same time reducing the error, ensuring confidentiality and integrity of cloud storage server. Thus, for data security in cloud, proposed algorithm proved to be more effective compared to existing algorithm. Stake holder can use this technique for securing the data in all fields

6.2 Scope for Further Study

Currently, designers are working more hard, to ensure people that cloud computing is the idea of the future. The current work focuses on developing a secure, scalable, transmission performance and safe retrieval of data in public cloud
environment. In future work can be extended by implementing the crypto-stegno technique in the community cloud and the performance of the same can be measured. In addition to it, the different SLA parameters that focus on improving cloud resource provider reputation level can be considered to improve the security. In order to attract the number of clients to the current model, an elegant user interface for crypto-stegno system can be designed after performing appropriate usability tests. The proposed crypto-stegno model and optimization algorithm can be integrated with open source virtualization like xen and kvm. QoS negotiation techniques can be implemented by improving the trustworthiness level of cloud service providers.