Chapter 8

Conclusion

This chapter concludes the results achieved through the thesis. The thesis goals defined in chapter 1 were related to the conceptual design presented in chapter 3, chapter 4, chapter 5, chapter 6 and chapter 7 of thesis. Together the conceptual design and implementations compromises the result of the thesis.

8.1 OUTCOMES ACHIEVED

Through the implementation of the access control schemes described in various chapters of the thesis numerous outcomes were achieved, where the major outcomes are described as follows:

1. Exploration of issues arising from existing access control techniques in the process of fine-grained cloud data access provision is made.

2. Practical deployment of newly deduced novel access control approaches to cloud computing environment that solves major security issues including fine-grained data access provision, data integrity, data privacy, forward and backward security assurances were made.

3. Finally an analysis and implementation of advanced security features with better system performance were made. An approach for reasoning the problems were made first, through which the newly developed technical solutions were deployed.
8.2 CONCLUSION

The highly dynamic and diverse nature of cloud computing demands the necessity for the establishment of security and access control schemes accompanying it. ABE is a public key based encryption technique that provides access privileges to the users built on their attributes. All over this research work we apply the concept of ABE over appropriate cloud deployment models, which leads to the development of novel access control and security endowment algorithms that overcomes delinquent data integrity, security, attribute revocation and affords fine-grained access rights to the individual users. An experimental set up is created using eucalyptus where all the newly proposed novel algorithms and system frameworks had been instigated. The experimental results depict the performance of the proposed scheme in edge to the existing techniques. All the algorithms and techniques provided through the entire research work are centered to the attainment of better security, integrity and fine-grained access of the outsourced data.

The overall concepts and techniques provided by the thesis are concluded as follows:

1. Some investigations on Novel access control techniques for cloud computing environment is made and solution to the problem of security, privacy, integrity issues associated with the cloud environment are provided.

2. The limitations of other traditional access policy models like DAC (Discretionary access control), MAC(mandatory access control) and RBAC (Role based access control) are identified and novel ac-
cess control schemes were designed to achieve flexible, scalable and fine-grained access control measures over the outsourced data in cloud computing.

3. The Proposed access control schemes were made to accommodate critical application deployment on cloud environment. Security breaches and crucial threats associated with the users of the system have been found and solved.

8.3 FUTURE WORK

The thesis presents suitable solution to existing access control schemes through the deployment of various newly defined novel access control approaches. As the need for cloud computing over safety of critical applications has increased tremendously, this work could be extended to meet the safety requirements of critical applications. Further this work can also be scaled in such a way to better suit the need of the users with high performance and security measures at lower costs. Further improvements in terms of energy efficiency can be addressed.