Chapter 5

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

Data outsourcing to from mobile devices to cloud servers is not a thing of future. In our everyday life we use many applications which store and retrieve data from remote cloud server to reduce load on resource constraint mobile device also there is a huge advantage come along such as centralization and sharing of data among multiple users. Group level sharing and authentication using ABE are studied vastly by numerous scholars till date but are limited to web users or web applications. There is very little or limited study on group level authorization and authentication of users in mobile cloud computing using CP-ABE mechanism resolving attribute revocation problem. It was tried to propose novel schemes in this regard so that the system model can be made more robust and resilient from unauthorized access. The complete research work is divided into four modules described below.

In module one of the research, a survey is done on different symmetric cryptographic techniques to find which one is best & efficient for mobile environment. It was found AES to be the well-suited algorithm and considered this algorithm as an encryption technique for future experiments.

In module two, an application design is proposed to make mobile user’s files more secured by using ABE in multi-cloud approach integrating RDA mechanism. For encryption we use ECIES algorithm which is combination of ECC and AES algorithm. Experiments proved the system to be efficient and reliable.

In module three, an application is designed to handle multi-keyword search on encrypted files on mobile cloud using ABE. Our architecture demonstrated soothing results where system seamlessly provides reliable service and user access control.

In module four, architecture is proposed based on which an application is designed to provide CP-ABE scheme in mobile computing. The proposed solution also provided fine grained access control for diverse user groups where user revocation and re-keying issues are vital to be taken care of. Experiments conducted on mobile app with web server integration shown fast and reliable results.
At last it can be summarized that due to dynamic nature of mobile devices and limitation of resources there is always a need of centralized platform where data can be outsourced and computational overhead can be shared. Web services in mobile computing help to achieve this task but again security is another major concern if data has to be shared within groups. ABE techniques integrated with fine grained access control can solve the security issues but need efficiency in terms of mobile computing. The above discussed proposed architectures can be of much value in maintaining equilibrium of sharing and security of data with performance. Mechanisms are proposed to have an efficient mobile based search on encrypted cloud data, data security with ABE in multi-cloud environment and architecture to solve attribute revocation problem. The solutions proposed are evaluated in real time devices and environment and are proved efficient on various parameters.

5.2 Future Works

As there is no limit for any research and the same may apply here. The system model proposed is tailored for group users in mobile cloud computing using ABE mechanism. We tested the model with one attribute assignment to each user, which forms groups based on common attributes and thus entire model contains multiple groups having multiple attributes. The model can be extended where a single user may have multiple attribute so that there could be more security of data.

For encryption purpose comparisons were made between symmetric algorithms keeping aside asymmetric algorithms. For extensions to this work asymmetric algorithms may also be studied to find out best efficient encryption mechanism on mobile. Also multiple encryption techniques can be combined to have additional security layer on data.