CHAPTER 7

CONCLUSIONS AND FUTURE WORK

7.1 CONCLUSIONS

Cloud computing offers numerous benefits to users. Due to its significant benefits, individuals and organizations are moving towards cloud technology. By moving data to cloud storage, users can avoid the burden of building and maintaining a storage infrastructure on their own. But, in spite of the significant benefits, the cloud model strive, with one main aspect that hinders its adoption widely, which is concern over security and privacy. But with proper adequate security measures, life in cloud will be more advantageous.

The prime objective of this thesis is to address cloud data security concerns and to mitigate concerns over confidentiality, authenticity, and integrity of data stored in cloud data storage. The analysis and results are summarized as follows.

An Adaptive Multilevel Security (AMLS) framework was designed from the perspective of data owner and was enforced to improve data confidentiality and to effectively secure the data outsourced to cloud data storage was provided. Several security challenges towards cloud data were discussed and a detailed review on various security measures was explicated. The responsibilities of a data owner in protecting cloud data and the need for Multilevel Security were also enumerated. Finally, to flaunt data classification with different encryption algorithms, it was illustrated using a private cloud environment deployed using OpenStack cloud operating system, in which, data
files ranging in different sizes are hosted and analysed and concluded that AES algorithm is felicitous for massive data stored in cloud storage.

An ECC based Adaptive and Secure Access Protocol (ECC-ASAP) was explicated which provided mutual authentication between data owner and data user and also ensured that the data stored in cloud storage is made available only to the authorized users thereby holding fine-grained access to resources. The protocol was designed to overcome attacks such as masquerade attack, impersonation attack, replay attack, and insider attack that were in the existing schemes. Also the protocol is designed in such a way that, an adversary cannot obtain any information regarding authentication and secret key details as all the communications were protected using encryption technique and session keys. From the security analysis, ECC-ASAP was proved to be secure in authorizing legitimate users and helps in providing fine-grained access to the resources.

An efficient and secure ECC based Digital Multi-Signature (ECC-DMS) Protocol was enumerated. Whenever the data is liable to manipulation, all the members of the security class collaboratively need to sign the data file, using which the data owner and other authorized members can verify the source of that data. The ECC-DMS protocol was designed to ensure the authenticity of data that is being shared between different security class members. Also, this protocol overcomes the insider attack and hence members of a group cannot impersonate other signers in the group. Also, the ECC-DMS protocol was proved to be efficient with reduced time complexity compared to other various digital multi-signature schemes.

An ECC based Provable Data Possession (ECC-PDP) Protocol with data dynamics for secure cloud storage was designed. The problems related with provable data possession schemes in cloud environment were outlined and
provable solutions to verify the integrity of data outsourced to cloud data storage were given. This protocol provides an efficient integrity verification method which helps data owner to perform stateless auditing. The integrity verification was done without retrieving the whole original data from cloud server, which minimizes communication overhead. The verifier can periodically effectively verify the integrity of data in cloud storage by challenging the cloud server to prove the data possession. Also, this protocol supports dynamic data operations at block level maintaining the same security assurance. The performance analysis proved the ECC-PDP protocol to be secure and efficient for cloud data storage.

Finally to conclude, the solutions and protocols provided in this thesis are secure, complete, and efficient which addresses and resolves concerns over Confidentiality, Authenticity, and Integrity of data in cloud data storage. The contributions of this thesis help data owners to achieve the promise of data security and convenient and flexible access to data while avoiding the threat of data misuse in cloud environment.

7.2 LIMITATIONS

The protocols specified in this thesis can be extended to preserve privacy in all aspects. The protocols in this research work are developed from the data owner’s perspective. But in case the data owner delegates part of his work to be done by any third party then these protocols may need to have minor modifications to prolong privacy.
7.3 FUTURE WORK

New security and privacy problems in the untrusted cloud environment can be investigated, as lot of new challenges arising day-to-day. Log analysis is not focused in this thesis. User behaviour analysis based on log entries can be done in such a way that it should help data owners to identify malicious users who is liable for data leakage. Based on the log entries any specific event that has occurred within a system or network must be identified so that data owner can analyse for the security attacks either that has happened or may happen in future. This review mechanism must be used to find when and which data should be reassessed for its sensitivity value and need to re-evaluate the adaptive security based on reassessed value. This kind of review mechanisms still enhances the security of outsourced data. Also from the log analysis, obsolete data can be identified and isolated and can be stored in low cost storage servers.