**CHAPTER- 9**

**CONCLUSION**

In this project, we study the forward security for public key searchable encryption, which means a new added encrypted data file cannot be searched by the search tokens generated before the encrypted data file. This security is urgently required for the public key searchable encryption schemes deployed in cloud storage, and can greatly reduce the privacy information leaked to a cloud server. As a solution, we propose a concrete scheme based on the 0-Encoding and 1- Encoding approach and give its security proof, further, we also show how to obtain a forward secure public key searchable encryption scheme from an attribute-based searchable encryption scheme by introducing a generic framework. Finally, we design experiments to illustrate the practicality of our proposed scheme in terms of encryption, token generation and search.