**CHAPTER- 9**

**CONCLUSION**

Combining protection against IKGA and efficiency is not trivial because the two properties are irreconcilable. In this paper, we have presented a new scheme called dual-server publickey authenticated encryption with keyword search (DPAEKS). The features of DPAEKS include: two non-colluding servers that are used to protect against IKGA and the data owner should be distributed with a pair of keys to authenticate the data. We developed a concrete construction of DPAEKS and proved its security. Finally, we implemented and evaluated the performance of the proposed scheme. The empirical results we obtained demonstrate that it is suitable for deployment in practical applications.