**CHAPTER-1**

**ABSTRACT**

To manage outsourced encrypted data sharing in clouds, attribute-based proxy re-encryption (ABPRE) has become an elegant primitive. In ABPRE, a cloud server can transform an original recipient’s ciphertext to a new one of a shared user’s. As the transformation is computation consuming, a malicious cloud server may return an incorrect re-encrypted ciphertext to save its computation resources. Moreover, a shared user may accuse the cloud server of returning an incorrect re9 encrypted ciphertext to refuse to pay the cost of using the cloud service. However, existing ABPRE schemes do not support a mechanism to achieve verifiability and fairness. In this paper, a novel verifiable and fair attribute-based proxy re-encryption (VF-ABPRE) scheme is introduced to support verifiability and fairness. The verifiability enables a shared user to verify whether the re-encrypted ciphertext returned by the server is correctand the fairness ensures a cloud server escape from malicious accusation if it has indeed conducted the re-encryption operation honestly. Additionally, we conduct a performance experimentto show the efficiency and practicality of the new VF-ABPREscheme.

Index Terms—Attribute-based proxy re-encryption, Data shar22 ing, Cloud computing, Verifiability, Fairness.