Key Policy-Attribute Based Fully Homomorphic Encryption (KP-ABFHE) Scheme for Securing Cloud Application in Multi-users Environment

Abstract

Recently, cloud technologies has become a cost-effective data solution among the small and medium-sized enterprises (SMEs). However, there is a raising concern on its security. This paper proposed the Key Policy-Attribute Based Fully Homomorphic Encryption (KP-ABFHE) scheme for providing an end-to end data protection in multi-users cloud environments. The proposed KP-ABFHE scheme is able to perform the computation while providing fine-grained access on the encrypted data. The proposed scheme is able to handle a monotonic access structure over a set of authorized attributes, without sacrificing the computation capabilities of homomorphic encryption. In addition, this paper proves that the proposed scheme is secure under a selective-set model with the hardness of Decision Ring-LWE\({_{d,q, \chi } }\) problem.