IMPROVING SECURITY AND PRIVACY ATTRIBUTE BASED DATA SHARING IN CLOUD COMPUTING

ABSTRACT

Data sharing is a convenient and economic service supplied by cloud computing. Data contents privacy also emerges from it since the data is outsourced to some cloud servers. To protect the valuable and sensitive information, various techniques are used to enhance access control on the shared data. In these techniques, Ciphertext policy attribute based encryption (CP-ABE) can make it more convenient and secure. Traditional CP-ABE focuses on data confidentiality merely; while the user's personal privacy protection is an important issue at present. CP-ABE with hidden access policy ensures data confidentiality and guarantees that user's privacy is not revealed as well. However, most of the existing schemes are inefficient in communication overhead and computation cost. Moreover, most of those works take no consideration on authority verification or the problem of privacy leakage in authority verification phase. To tackle the problems mentioned above, a privacy preserving CP-ABE scheme with efficient authority verification is introduced in this project. Additionally, the secret keys of it achieve constant size. Meanwhile, the proposed scheme achieves the selective security under the decisional *n*-BDHE problem and decisional linear assumption. The computational results confirm the merits of the presented scheme.