Authentication and Key Agreement based on Anonymous Identity for Peer-to-Peer Cloud

Cross-cloud data migration is one of the prevailing challenges faced by mobile users, which is an essential process when users change their mobile phones to a different provider. However, due to the insufficient local storage and computational capabilities of the smart phones, it is often very difficult for users to backup all data from the original cloud servers to their mobile phones in order to further upload the downloaded data to the new cloud provider. To solve this problem, we propose an efficient data migration model between cloud providers and construct a mutual authentication and key agreement scheme based on elliptic curve certificate-free cryptography for peer-to-peer cloud. The proposed scheme helps to develop trust between different cloud providers and lays a foundation for the realization of cross-cloud data migration. Mathematical verification and security correctness of our scheme is evaluated against notable existing schemes of data migration, which demonstrate that our proposed scheme exhibits a better performance than other state-of-the-art scheme in terms of the achieved reduction in both the computational and communication cost.

Domain: Cloud Computing
Technology: Java