abtechchennai@gmail.com
www.abtechnologies.in
9840511458

IDENTITY-BASED PRIVACY PRESERVING REMOTE DATA INTEGRITY CHECKING FOR CLOUD STORAGE

ABSTRACT

Although cloud storage service enables people easily maintain and manage amounts of data with lower cost, it cannot ensure the integrity of people's data. In order to audit the correctness of the data without downloading them, many remote data integrity checking (RDIC) schemes have been presented. Most existing schemes ignore the important issue of data privacy preserving and suffer from complicated certificate management derived from public key infrastructure. To overcome these shortcomings, this project proposes a new Identity-based RDIC scheme that makes use of homomorphic verifiable tag to decrease the system complexity. The original data in proof are masked by random integer addition, which protects the verifier from obtaining any knowledge about the data during the integrity checking process. Our scheme is proved secure under the assumption of computational Diffie–Hellman problem.