abtechchennai@gmail.com
www.abtechnologies.in
9840511458

EFFICIENT PROOFS OF RETRIEVABILITY WITH PUBLIC VERIFIABILITY FOR DYNAMIC CLOUD STORAGE

ABSTRACT

Cloud service providers offer various facilities to their clients. The clients with limited resources opt for some of these facilities. They can outsource their bulk data to the cloud server. The cloud server maintains these data in lieu of monetary benefits. However, a malicious cloud server might delete some of these data to save some space and offer this extra amount of storage to another client. Therefore, the client might not retrieve her file (or some portions of it) as often as needed. Proofs of retrievability (PoR) provide an assurance to the client that the server is actually storing all of her data appropriately and they can be retrieved at any point of time. In a dynamic PoR scheme, the client can update her data after she uploads them to the cloud server. Moreover, in publicly verifiable PoR schemes, the client can delegate her auditing task to some third party specialized for this purpose. In this work, we exploit the homomorphic hashing technique to design a publicly verifiable dynamic PoR scheme that is more efficient (in terms of bandwidth required between the client and the server) than the "state-of-the-art" publicly verifiable dynamic PoR scheme. We also analyze security and performance of our scheme.