TECHNOLOGIES

abtechchennai@gmail.com
www.abtechnologies.in
9840511458

A PARALLEL AND FORWARD PRIVATE SEARCHABLE PUBLIC-KEY ENCRYPTION FOR CLOUD-BASED DATA SHARING

ABSTRACT

Data sharing through the cloud is flourishing with the development of cloud computing technology. The new wave of technology will also give rise to new security challenges, particularly the data confidentiality in cloud-based sharing applications. Searchable encryption is considered as one of the most promising solutions for balancing data confidentiality and usability. However, most existing searchable encryption schemes cannot simultaneously satisfy requirements for both high search efficiency and strong security due to lack of some must have properties, such as parallel search and forward security. This project proposes a variant searchable encryption with parallelism and forward privacy, namely the parallel and forward private searchable public-key encryption (PFP-SPE). PFP-SPE scheme achieves both the parallelism and forward privacy at the expense of slightly higher storage costs. PFP-SPE has similar search efficiency with that of some searchable symmetric encryption schemes but no key distribution problem. The security analysis and the performance evaluation on a real world dataset demonstrate that the proposed scheme is suitable for practical application.