AK Tech Training and Placements

Transform Dreams into Reality

A Parallel and Forward Private Searchable Public-Key Encryption for Cloud-Based Data Sharing

Data sharing through the cloud is evolving with the development of cloud computing technology. New technology leads to new security challenges, especially data privacy in cloud-based sharing applications. Searchable encryption is considered one of the best solutions to balance data privacy and usability. However, most existing searchable encryption schemes do not meet the requirements for both high search capability and robust security simultaneously due to the lack of some must-have features such as parallel search and forward security.We propose variant searchable encryption with parallel and forward privacy, namely parallel and forward private searchable public-key encryption. The PFP-SPE scheme achieves both parallelism and forward privacy at the expense of slightly higher storage costs. PFP-SPE has similar search capability with some searchable symmetric encryption schemes, but no key distribution issue.

Domain: Cloud Computing
Technology: Java