AK Tech Training and Placements

Transform Dreams into Reality

Privacy Preserving Multi-keyword Searchable Encryption for Distributed Systems

As cloud storage has been widely adopted in various applications, how to protect data privacy while allowing efficient data search and retrieval in a distributed environment remains a challenging research problem. Existing searchable encryption schemes are still inadequate on desired functionality and security/privacy perspectives. Specifically, supporting multi-keyword search under the multi-user setting, hiding search pattern and access pattern, and resisting keyword guessing attacks (KGA) are the most challenging tasks. In this application, we present a new searchable encryption scheme that addresses the above problems simultaneously, which makes it practical to be adopted in distributed systems. It not only enables multi-keyword search over encrypted data under a multi-writer/multi reader setting but also guarantees the data and search pattern privacy. We provide a subset decision mechanism is also designed as the core technique underlying our scheme and can be further used in applications other than keyword search. Finally, we prove the security and evaluate the computational and communication efficiency of our scheme to demonstrate its practicality

Domain: Cloud Computing
Technology: Java