

**User Differentiated Verifiable File Search on the Cloud**

**Abstract:**

Cloud storage security has been gaining research interest in recent years. Although considerable work has been conducted on verifying the integrity of the outsourced data in the cloud, how to efficiently verify the file search results returned from the cloud is still a challenge to be resolved. Towards this direction, we tackle the verifiable file search problem in this paper. We formulate and solve this problem by proposing two protocols. The first protocol enables verifying the correctness of the file search result when all users have the same security privilege in accessing the outsourced data. The second protocol, which builds on the first protocol, further enables user differentiation, i.e., different users can only access files that fit their security privileges. In our protocols, we employ two key strategies in enabling file search verifiability. One is to separate all possible filenames into two finite sets and the other is to embed some secret information in the outsourced data. Further, we leverage the key chaining and recursion mechanisms to enable user differentiation. We have conducted experiments to validate the effectiveness of our proposed protocols. Our results show that both protocols are efficient in terms of computation, storage, and communication cost.