Fast and Scalable Range Query Processing With Strong Privacy Protection
for Cloud Computing

Privacy has been the key road block to cloud computing as clouds may not be fully trusted. This paper is concerned with the problem of privacy-preserving range query processing on clouds. Prior schemes are weak in privacy protection as they cannot achieve index indistinguishability, and therefore allow the cloud to statistically estimate the values of data and queries using domain knowledge and history query results. In this paper, we propose the first range query processing scheme that achieves index indistinguishability under the indistinguishability against chosen keyword attack (IND-CKA). Our key idea is to organize indexing elements in a complete binary tree called PBtree, which satisfies structure indistinguishability (i.e., two sets of data items have the same PBtree structure if and only if the two sets have the same number of data items) and node indistinguishability (i.e., the values of PBtree nodes are completely random and have no statistical meaning). We prove that our scheme is secure under the widely adopted IND-CKA security model. We propose two algorithms, namely PBtree traversal width minimization and PBtree traversal depth minimization, to improve query processing efficiency. We prove that the worst-case complexity of our query processing algorithm using PBtree is, where the total number of data items is and is the set of data items in the query result. We implemented and evaluated our scheme on a real-world dataset with 5 million items. For example, for a query whose results contain 10 data items, it takes only 0.17 ms.