Ph: 9585554590, 9585554599
Email: support@salemsmartreach.com
URL: www.salemsmartreach.com

Secure Two-Party Differentially Private Data Release for Vertically Partitioned Data

Abstract:

Privacy-preserving data publishing addresses the problem of disclosing sensitive data when mining for useful information. Among the existing privacy models, ϵ-differential privacy provides one of the strongest privacy guarantees. In this paper, we address the problem of private data publishing, where different attributes for the same set of individuals are held by two parties. In particular, we present an algorithm for differentially private data release for vertically partitioned data between two parties in the semihonest adversary model. To achieve this, we first present a two-party protocol for the exponential mechanism. This protocol can be used as a subprotocol by any other algorithm that requires the exponential mechanism in a distributed setting. Furthermore, we propose a two-party algorithm that releases differentially private data in a secure way according to the definition of secure multiparty computation. Experimental results on real-life data suggest that the proposed algorithm can effectively preserve information for a data mining task.