ABSTRACT

In the big data era, organizations continuously collect vast amounts of sensitive information, and a key challenge is to get meaningful analytical results without compromising privacy. As a gold standard for private data analysis, differential privacy (DP) has garnered significant attention from both academia and industry. Informally speaking, DP requires that query results are indistinguishable regardless of whether any particular individual’s data is included or not in the database thus we cannot infer any individual’s information through the query result. Noise injection is inherently necessary for this goal. Although DP is widely researched in all kinds of data science areas, many DP mechanisms do not provide a practical utility (error level) in real-world applications. The primary challenge is that traditional DP methods often set a universal limit on individual contributions to queries and add noise in proportion to this limit. This results in a consistent error level on every instance, which can be very high in practice. To address this, I advocate for a novel concept: instance-optimal error, which minimizes error for each specific instance rather than universally. This “paradigm shift” in DP design enhances practical utility significantly. My focus is on two areas: developing a practical DP SQL query engine and designing practical DP solutions for artificial intelligence.