Review: Database Access Control & Privacy: Is There A Common Ground?

Layla Pournajaf
Department of Mathematics and Computer Science
Emory University

Summary  Surajit Chaudhuri et. al in the paper ”Database Access Control & Privacy: Is There A Common Ground?” proposed a method to integrate differential privacy with existing policy-based access control methods. Their method does not change the existing building blocks of the database or database management system, it rather uses the query-rewriting approach which is applied on original database and a new type of views (DPVs) using the existing authorization methods. DPVs (Differentially private views) are defined as noisy views of combined unauthorized and authorized data that can be used to answer combined queries. They support several aggregation functions such as min, sum, count, and key-key join to produce differentially private noisy views.

Positive Points

1. This is one of the first works that integrates differential privacy into commercial authorization system using SQL.

2. The paper is straight forward and easy to follow.

3. The method does not change the existing database systems and takes advantage of commercially used tools and frameworks.

Negative Points
1. They do not discuss how utility is affected by this method.

2. The paper does not provide any experiment/analysis that evaluates the performance of the work regarding to the query response time and/or space requirements.

Discussion Points and Questions

1. Noisy views need to be computed for a various type of data aggregation over various data tables for different users. If they materialize these views it might be space costly and if they do it on the fly it might be time consuming. How do they address this issue?

2. They do not mention how the parameters of differential privacy is chosen in this system. For example how they assign privacy budget to users?