Differential Privacy Preserving Regression Analysis and Deep Learning

Xintao Wu
University of Arkansas,USA
xintaowu@uark.edu

ABSTRACT

Many data mining and machine learning methods such as regression models often involve optimization of objective functions. The functional mechanism (FM), which perturbs coefficients of the polynomial representation of the objective function, has been shown as an effective way to achieve differential privacy. Although the learned model guarantees protection against attempts to infer whether a subject was included in the training set, it is not designed to protect attribute privacy when model inversion attacks are launched. In model inversion attacks, an adversary uses the released model to make predictions of sensitive attributes of a target individual when some background information is available. In the first part of this talk, we present an approach which leverages the FM but effectively balances the privacy budget for sensitive and non-sensitive attributes in learning the model. As a result, the approach can effectively prevent model inversion attacks and retain model utility while preserving privacy. In the second part of this talk, we concentrate on recent research on privacy preserving deep learning. In particular, we present the differential privacy preserving deep Auto-encoder based on the FM. Finally we present challenges and findings when applying the developed techniques in healthcare and genome wide association studies.

Keywords

Differential privacy; regression; deep learning

Biography

Dr. Xintao Wu is the professor and the Charles D. Morgan/Acxiom Endowed Graduate Research Chair in Database in Computer Science and Computer Engineering Department at University of Arkansas. He was a faculty member in College of Computing and Informatics at the University of North Carolina at Charlotte from 2001 to 2014. Dr. Wu's major research interests include data mining, privacy and security, database application testing and big data analysis. His recent research work has been to develop privacy preserving techniques for mining tabular data, social network data, healthcare data, and GWAS data and develop spectral analysis based fraud detection techniques in social networks. Dr. Wu has published over 90 scholarly papers. He and his students received several awards including a PAKDD'09 Best Student Paper Runner-up Award, WISE'12 Challenge Runner-up Award, PAKDD'13 Best Application Paper Award, and BIBM'13 Best Paper Award. Dr. Wu has served on editorial boards of several international journals and frequently served on NSF review panels and program committees of top international conferences, including ACM KDD, CIKM, IEEE ICDM, SIAM SDM, PKDD, and PAKDD. Dr. Wu is a recipient of NSF CAREER Award (2006), Excellence in Undergraduate Teaching Award (2005), and Outstanding Faculty Research Award (2009) from College of Computing and Informatics at UNC Charlotte.