1145-VN-2993 **Kevin Li*** (likevin6688@gmail.com), **Mingyang Zhang** (zhangbruin24@g.ucla.edu) and **Xiaodi Wang** (wangx@wcsu.edu). *Privacy-preserving support vector regression and deep learning.*

Today, every moment huge amount of personal information is collected, stored, used in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. These issues may arise from a wide range of sources such as in healthcare records, criminal investigations and proceedings, web surfing behavior using persistent cookies, academic research, and financial transactions. Data analysis with privacy-preserving can be regarded as statistical disclosure control, private data analysis, and privacy-preserving data-mining. To achieve the goal, some robust concepts of privacy-preserving such as k-anonymity and l-diversity have been proposed. However, even these methods cannot prevent private information leaking from attacks. In an extreme case, the attacker might know the contents of all but one of the rows in the set . To combat such background attacks, Dwork proposed concept of Differential privacy. In this research, we'll private an algorithm that will allow multiple parties to jointly apply support vector regression and deep learning models for a given objective without sharing their input datasets so that differential privacy will be achieved. (Received September 26, 2018)