Abstract

Data mining tool discovers valuable knowledge [1] from the huge volumes of data. The knowledge discovered is treated as an important asset and constructive feature for the growth of business. Inspite of its significant analytical capability the data mining tools have some limitations to its capabilities. The data mining techniques not only derive interesting patterns but
A Novel Framework to Improve the Quality of Additive Perturbation Technique

can also reveal highly sensitive information available in the database. Publicizing such data for analysis purpose opens new threats to individual privacy. The threat to privacy [12] due to data mining is the highly concerned issue from the society. Privacy preserving data mining [2] is new research area in data mining, which presents solutions to privacy problems that occur during the data mining process. The main motive of PPDM technique is to obtain valid data mining results without access to the original sensitive information. In this paper we discussed the problems associated with privacy preservation of sensitive information due to basic randomized additive perturbation technique. We proposed a novel framework to enhance the performance and quality of basic additive perturbation technique. This framework not only preserves the privacy of sensitive information, but also gives modified database valid for various analysis purpose.

Reference

- Kantarcioglu, M., Jin, J. and Clifton C. 2004. When do data mining results violate privacy?. In Proceedings ACM SIGKDD international conference on Knowledge discovery and data mining,

Index Terms
A Novel Framework to Improve the Quality of Additive Perturbation Technique

Computer Science  Security

Key words  
Data mining  privacy  privacy preserving data
mining