Abstract

An important problem in publishing the data is privately held data about individuals without revealing the sensitive information about them. Several anonymization techniques, such as suppression, bucketization and slicing have been designed for privacy preservation in microdata publishing. Suppression involves not releasing a value at all it leads to the utility loss while the anonymized table may use by the data miners. Bucketization does not prevent membership disclosure and does not apply for data that do not have a clear separation between quasi-identifying attributes and sensitive attributes. On the other hand slicing, this partitions the data both horizontally and vertically. Slicing preserves better data utility than generalization and
can be used for membership disclosure protection. But in the slicing each attribute consider only single column. This releases more attribute correlations and it leads to a secrecy loss in privacy. An effective slicing is introduced in this paper to show how slicing can be performed with suppression in the attributes which have similar values in the different tuples and an efficient algorithm for computing the sliced data that obey the l-diversity requirement.

References

- C. Aggarwal, 2005 On k-Anonymity and the Curse of Dimensionality, Proc. Int'l Conf. Very Large Data Bases (VLDB), pp. 901-909

Index Terms

Computer Science
Security
Keywords
Privacy Preservation  Suppression  Slicing  Suppression Slicing