Abstract

For privacy preserving data publishing many anonymization techniques such as generalization and bucketization have been designed. Next, a novel technique is presented, called slicing to
have a clear separation between quasi-identifying attributes. It partitions the data both horizontally and vertically and can be used to prevent membership disclosure protection. For anonymizing horizontally partitioned data at multiple data providers, the collaborative data publishing problem is considered. A new type of "insider attack" is being introduced by colluding data providers who may use their own data records with the external background knowledge to infer the data records contributed by other data providers. m-privacy is introduced which guarantees that the anonymized data satisfies a given privacy constraint against any group of up to m colluding data providers. A data provider-aware anonymization algorithm is presented with m-privacy checking strategies to ensure high utility and efficiency. This approach achieves better utility and efficiency in real-life datasets.

References

An Efficient Collaborative Data Publishing by M-Privacy Technique


Index Terms

Computer Science

Data Mining

Keywords

M-privacy  Quasi-identifying Attributes  M-adversary  T-closeness  L-diversity  K-anonymity.