Abstract

Protecting individual's privacy has become a major concern among privacy research community. Many frameworks and privacy principles were proposed for protecting the privacy of the data that is being released to the public for mining purpose. k-anonymization was the most popular among the proposed techniques in which the sensitive association between the sensitive attributes and their corresponding identifiers are de-associated. In this paper, we proposed an enhanced k-anonymity technique by using Minimum Spanning Tree (MST) partitioning approach. In this technique we disclose the information of the individuals pertaining to minimum group size i.e., k. We achieve this technique in two phases. During the first phase, MST for the given dataset is partitioned to generate equivalence classes and in the subsequent phase whether the equivalence class size is achieved to that of the minimum group size k is verified. Our approach resulted in achieving the optimal anonymization along with data utility. We showed the efficacy of our proposed technique by running a series of experiments in terms of information loss to show that our technique adheres to the quality of the anonymized data.
Achieving k-anonymity using Minimum Spanning Tree based Partitioning

- Jiuyong, Li. , Raymond Chi-Wing, W. , Ada Wai-Chee Fu and Jian Pei.  2006. Achieving k-Anonymity by clustering in Attribute Hierarchical Structures, In Proceeding of the 8th International Conference on Data Warehousing and Knowledge Discovery, Krakow, Poland, pp. 405-416.
- Samarati, P.  2001. Protecting respondent’s identities in microdata Release, In
IEEE Transactions on Knowledge and Data Engineering, Vol. 13 (6). pp. 1010-1027
- Graham, C., Srivastava, D. 2011. Ting Yu and Qing Zhang, Anonymizing Bipartite graph data using safe groupings, VLDB journal, pp. 115-139.

Index Terms
Computer Science
Algorithms

Keywords
Privacy Anonymisation Hierarchical distance Minimum Spanning Tree Inflexion point