Abstract

Development of online social networks and publication of social network data has led to the risk of leakage of confidential information of individuals. This requires the preservation of privacy before such network data is published by service providers. Privacy in online social networks data has been of utmost concern in recent years. Hence, the research in this field is still in its early years. Several published academic studies have proposed solutions for providing privacy of tabular micro-data. But those techniques cannot be straight forwardly applied to social network data as social network is a complex graphical structure of vertices and edges. Techniques like k-anonymity, its variants, L-diversity have been applied to social network data. Integrated technique of K-anonymity & L-diversity has also been developed to secure privacy of social network data in a better way.

References

- Jaideep Srivastava, Muhammad A. Ahmad, Nishith Pathak, David Kuo-Wei Hsu, "Data mining based social network analysis from online behavior," SIAM conference on Data Mining, 2008.
Privacy Preserving Techniques in Social Networks Data Publishing - A Review

- Mingxuan Yuan, Lei Chen, Philip S. Yu, Ting Yu, "Protecting Sensitive Labels in..."
- Roy Ford, Traian Marius Truta, and Alina Campan, “P-Sensitive K-Anonymity for Social Networks”.
- Aaron Beach, Mike Gartrell, Richard Han, “q-Anon: Rethinking Anonymity for Social Networks”, In Proc. of IEEE Second International Conference on Social Computing
Privacy Preserving Techniques in Social Networks Data Publishing - A Review

(SocialCom), Minneapolis, MN, pp 185 – 192, 2010.

Index Terms

Computer Science
Security

Keywords

Privacy models  K-anonymity  L-diversity  t-closeness.