Abstract

Privacy has become crucial in knowledge based applications. Proper integration of individual privacy is essential for data mining operations. This privacy based data mining is important for sectors like Healthcare, Pharmaceuticals, Research, and Security Service Providers, to name a few. The main categorization of Privacy Preserving Data Mining (PPDM) techniques falls into Perturbation, Secure Sum Computations and Cryptographic based techniques. There exist tradeoffs between privacy preservation and information loss for generalized solutions. The authors of the paper present an extensive survey of PPDM techniques, their classification and give a preliminary implication of technique to be used under specific scenarios.

References

2. Li Liu, Murat Kantarcioglu and Bhavani Thuraisingham, “The applicability of the


5. Tianchong Li, Ninghui Li, “Towards Optimal k-anonymization”, Data & Knowledge Engineering, 2008 Elsevier. 303


Privacy Preserving Data Mining: Techniques, Classification and Implications - A Survey


25. Benny Pinkas, “Cryptographic techniques for privacy preserving data mining”,


34. Benjamin C. M. Fung, Ke Wang, Lingyu Wang, Patrick C.K. Hung, “Privacy-preserving data publishing for cluster analysis”, Data & Knowledge Engineering 68


36. Asmaa H.Rashid and Prof.dr. Abd-Fatth Hegazy, “Protect Privacy of Medical Informatics using K-Anonymization Model”, IEEE Explore


46. Tsiafoulis, S.G. Zorkadis, V.C., 2010, A Neural Network Clustering Based Algorithm for Privacy Preserving Data Mining, International Conference on Computational Intelligence and Security (CIS), 2010, pp: 401-405

Index Terms

Computer Science
Information Sciences
Keywords

PPDM, Perturbation, Cryptography, SMC, Randomization, Condensation, Anonymization