Abstract

Confidentiality of data or resources is of primary importance in Privacy Preserving Data Mining (PPDM) Systems. The research work presented through this paper discusses the PPDM model in which the privacy of data transacted amongst the various Data Custodians involved is highlighted. The data available with each data custodian is assumed to be horizontally portioned. The proposed model considers the C5.0 algorithm for data mining and classification rule generation due to its advances and classification accuracy over its predecessors. Privacy of the data transacted or secure multiparty computation is achieved by using the commutative RSA cryptography scheme. The proposed model is compared with the existing secure group communication techniques like Secure Lock and Asynchronous Control Polynomial in terms of computational efficiency. Furthermore the privacy preserving feature of the proposed scheme is proved in terms of the computational indistinguishability of the data transacted amongst the varied data custodians involved discussed in the paper.
- J. Vaidya and C. W. Clifton, "Privacy preserving association rule mining in vertically partitioned data," in Proc. ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining, 2002.
- J. Vaidya and C. Clifton, "Privacy-preserving k-means clustering over vertically partitioned data," in Proc. ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining, 2003.
Conference. 4-7 Jan. 2011.
- Christian Cachin and Jan Camenisch, IBM Research–Zurich, "Encrypting Keys Securely," IEEE COMPUTER AND RELIABILITY SOCIETIES. 1540-7993/10/
JULY/AUGUST 2010.

**Index Terms**

Computer Science  
Artificial Intelligence

**Keywords**

Privacy Preserving Data Mining  
Semi Honest Model  
Secure Multiparty Computation  
Commutative RSA  
C5.0  
Data mining Algorithm

Classification Rules