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.
Secure Multi Party Computation Technique for Classification Rule Sharing

- J. Vaidya and C. Clifton, &quot;Privacy-preserving k-means clustering over vertically partitioned data,&quot; in Proc. ACM SIGKDD Int&apos;s Conf. on Knowledge Discovery and Data Mining, 2003.  
- D. Agrawal and C. C. Aggarwal, &quot;On the design and quantification of privacy preserving data mining algorithms,&quot; in Proceeding of the 20th ACM Symposium on Principles of Database Systems, Santa Barbara, California.  
- K. Chen and L. Liu, &quot;Privacy preserving data classification with rotation perturbation,&quot; in Proc. Int&apos;s Conf. on Data Mining, 2005.  
- S. Papadimitriou, F. Li, G. Kollios, and P. S. Yu, &quot;Time series compressibility and privacy,&quot; in Proc. Int&apos;s Conf. on Very Large Data Bases, 2007.  
- A. Evfimievski, R. Srikannt, R. Agrawal, and J. Gehrke, &quot;Privacy preserving mining of association rules,&quot; in ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2002.  
- W. Du and Z. Zhan, &quot;Using randomized response techniques for privacy-preserving data mining,&quot; in Proc. ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2003.  
- R. Agrawal, R. Srikannt, and D. Thomas, &quot;Privacy preserving OLAP,&quot; in Proc. ACM SIGMOD Int&apos;s Conf. on Management of Data, 2005.  
- Tamir Tassa,&quot;Secure Mining of Association Rules in Horizontally Distributed Databases;&quot; 2011  
- C. C. Aggarwal and P. S. Yu, &quot;A condensation approach to privacy preserving data mining,&quot; in Proc. Int&apos;s Conf. on Extending Database Technology (EDBT), 2004.  
- Slava Kisilevich, Lior Rokach, Yuval Elovici and Bracha Shapira,&quot;Efficient Multidimensional Suppression for K-Anonymity&quot;; IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 22, NO. 3, MARCH 2010  
- X. Zou, Y. -S. Dai, and E. Bertino, &quot;A practical and flexible key management mechanism for trusted collaborative computing,&quot; Proceedings of INFOCOM&apos;s;08, Phoenix, AZ, USA, pp. 1211–1219, Apr. 2008  
- Xukai Zou, Mingrui Qi, and Yan Sui. &quot;A New Scheme for Anonymous Secure Group Communication;&quot; System Sciences (HICSS), 2011 44th Hawaii International
Secure Multi Party Computation Technique for Classification Rule Sharing

Conference. 4-7 Jan. 2011.
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