系统工程与电子技术 2012, 34(11) 2390-2395 DOI: 10.3969/j.issn.1001-506X.2012.11.35 ISSN: 1001-506X CN: 11-2422/TN

软件、算法与仿真

基于SMC的分布式隐私保护数据发布研究

方炜炜, 周长胜, 贾艳萍, 刘亚辉

北京信息科技大学信息中心, 北京 100192

摘要：

针对垂直分布式存储结构的隐私保护数据发布问题，基于元组等价群的概念给出全局k-匿名化的定义和充要条件，采用集合多项式表示方法求解出全局元组ID等价群；并基于多方安全计算的同态加密协议构建了具有隐私性、准确性和公平性的分布式隐私保护k-匿名模型，从而实现了各微数据提供方不泄露本地隐私信息的前提下由半可信第三发布方发布出可供统计分析和数据挖掘等需求的真实有效数据集。实验结果表明,该模型具有很好的安全性、准确性和适用性。

关键词： 隐私保护数据发布 多方安全计算 匿名 同态加密

Research on distributed privacy preserving data publishing based on SMC

FANG Wei-wei, ZHOU Chang-sheng, JIA Yan-ping, LIU Ya-hui

Computer Center, Beijing Information Science and Technology University, Beijing 100192, China

Abstract:

To solve the privacy-preserving data publishing problem in context of vertical distribution, the definition of global k-anonymity and its necessary and sufficient conditions are given based on the concept of equivalent groups of tuples, the global equivalent groups of tuples are solved by using a polynomial representation method, a distributed privacy preserving k-anonymity model which has the character of privacy, accuracy and fairness by applying the set polynomial indication method and homomorphic encryption protocol based on secure multi-party computation is proposed. The model can help each data owner to securely publish real and affect data set for statistical analyzing and data mining without revealing sensitive original information. Experiments demonstrate that this model can provide the good capability of security, accuracy and efficiency.

Keywords: privacy preserving data publishing (PPDP) secure multi-party computation (SMC) anonymity homomorphic encryption

收稿日期 修回日期 网络版发布日期

DOI: 10.3969/j.issn.1001-506X.2012.11.35

基金项目:

通讯作者:

作者简介:

作者Email:

参考文献：

本刊中的类似文章

1. 郭昆，张岐山.基于灰关联分析的K匿名方法及其在聚类中的应用[J]. 系统工程与电子技术, 2011,33(9): 2139-2143

2. 方炜炜, 杨炳儒, 夏红科.基于SMC的隐私保护聚类模型[J]. 系统工程与电子技术, 2012,34(7): 1505-1510