基于同态加密的分布式隐私保护线性回归分析模型

李 娟，马 飞
(北方民族大学 计算机科学与工程学院，宁夏 银川 750021)

摘 要：线性回归是对数据进行统计分析的重要方法之一，但对具有隐私保护的分布式多数据源线性回归分析的研究还较少．针对该问题，利用加性同态加密，提出了一种在非信任的分布式环境下具有隐私保护的协作线性回归分析模型．该模型充分利用分布式环境的计算能力，由各数据源端与服务器端协作进行线性回归参数的计算，各数据源的敏感数据在整个分析过程中都处于保密状态．最后分析了模型在半诚实模式下的安全性，并对所实现模型进行了性能测试．

关键词：隐私保护；同态加密；线性回归；半诚实模式

中图分类号：TP309.7　**文献标识码**：A　**文章编号**：1000－7180(2016)01－0110－04

A Model on Distributed Privacy Preserving Linear Regression Analysis Based on Homomorphic Encryption

LI Juan, MA Fei
(School of Computer Science and Engineering, Beifang University of Nationalities, Yinchuan 750021, China)

Abstract: Linear regression is one of the important methods of statistical analysis, but the research on linear regression analysis with privacy preserving for multiple data source in distributed environment is relatively less. To solve this problem ,by using additive homomorphic encryption, a model on collaborative linear regression analysis with privacy preserving in non-trusted distributed environment is presented. The model makes full use of the calculating ability of distributed environment, the clients and statistical server collaboratively calculate linear regression parameters, and the sensitive data of each data source are protected in analysis process. Finally, the security of model is discussed in Semi- Honest Mode, and the performance of model is tested.

Key words: Privacy Preserving; homomorphic encryption; linear regression; Semi-Honest Mode

作者简介：

李 娟 女，(1975-)，硕士，副教授．研究方向为云计算、网络安全、社交网络与隐私保护．

马 飞 男，(1976-)，博士，副教授．研究方向为数据挖掘、云计算，社交网络分析与隐私保护．

E-mail：feixiangflying33@nxu.edu.cn.