Contents lists available at ScienceDirect

Information Systems

journal homepage: www.elsevier.com/locate/is

Privacy preserving mechanisms for optimizing cross-organizational collaborative decisions based on the Karmarkar algorithm

Hui Zhu[a], Hongwei Liu[b], Carol XJ Ou[c], Robert M. Davison[d,*], Zherui Yang[e]

[a] School of Management Guangzhou University, Guangzhou, China
[b] School of Management Guangdong University of Technology, China
[c] Department of Management Tilburg University, The Netherlands
[d] Department of Information Systems City University of Hong Kong, Hong Kong
[e] Department of Technology and Operations Management Rotterdam School of Management Erasmus University Rotterdam The Netherlands

ARTICLE INFO

Article history:
Received 2 February 2016
Revised 9 August 2017
Accepted 18 October 2017

Keywords:
Collaborative optimization
Privacy preserving mechanisms
The Karmarkar algorithm
Secure Multi-Party Computation (SMC)
Secure Two-Party Computation (STC)

ABSTRACT

Cross-organizational collaborative decision-making involves a great deal of private information which companies are often reluctant to disclose, even when they need to analyze data collaboratively. The lack of effective privacy-preserving mechanisms for optimizing cross-organizational collaborative decisions has become a challenge for both researchers and practitioners. It is even more challenging in the era of big data, since data encryption and decryption inevitably increase the complexity of calculation. In order to address this issue, in this study we introduce the Karmarkar algorithm as a way of dealing with the privacy-preserving distributed linear programming (LP) needed for secure multi-party computation (SMC) and secure two-party computation (STC) in scenarios characterised by mutual distrust and semi-honest participants without the aid of a trusted third party. We conduct two simulations to test the effectiveness and efficiency of the proposed protocols by revising the Karmarkar algorithm. The first simulation indicates that the proposed protocol can obtain the same outcome values compared to no-encryption algorithms. Our second simulation shows that the computational time in the proposed protocol can be reduced, especially for a high-dimensional constraint matrix (e.g., from 100 × 100 to 1000 × 1000). As such, we demonstrate the effectiveness and efficiency that can be achieved in the revised Karmarkar algorithm when it is applied in SMC. The proposed protocols can be used for collaborative optimization as well as privacy protection. Our simulations highlight the efficiency of the proposed protocols for large data sets in particular.

1. Introduction

The advent of big data analytics has enabled the measurement and analysis of variables that could only be measured with difficulty in the past, such as public sentiment, opinion, actual behavior and personal data. In order to optimize inter-organizational collaborative decision-making, the involved parties need to share and analyze both their own data, as well as data from their business partners and even competitors [1]. However, the involved organizations may be reluctant to share and disclose such information [2–4]. This leads to a significant challenge for researchers and practitioners [5]: How can organizations reconcile the contradictions between optimizing decision making based on the shared information and simultaneously protecting the individual private information contained in the shared data?

For instance, collaborative supply chain management emphasizes multi-party participation (e.g., among material suppliers, manufacturers, logistics providers and distributors) in order to both optimize supply chain arrangements as a whole [6]and achieve smooth collaboration between the two adjacent nodes of a supply chain in demand forecasting [7]. This multi-party participation can eliminate potential demand variations [8]. Similarly, a collaborative center based on distribution networks was proposed as a solution to harmonize third-party logistics providers who coordinated shipments between suppliers and customers [9]. However, for these distributed linear programming (LP) problems, supply chain participants are often reluctant to share their private information directly with third parties, considering the high level of risk that the private information may be disseminated to other unauthorised parties. As a result, concerns about information security

[*] Corresponding author.
E-mail addresses: zhuhui@gzhu.edu.cn (H. Zhu), hwliu@gdut.edu.cn (H. Liu), carol.ou@uvt.nl (C.X. Ou), isrobert@cityu.edu.hk (R.M. Davison), yang@rsm.nl (Z. Yang).

https://doi.org/10.1016/j.is.2017.10.008
0306-4379/© 2017 Elsevier Ltd. All rights reserved.

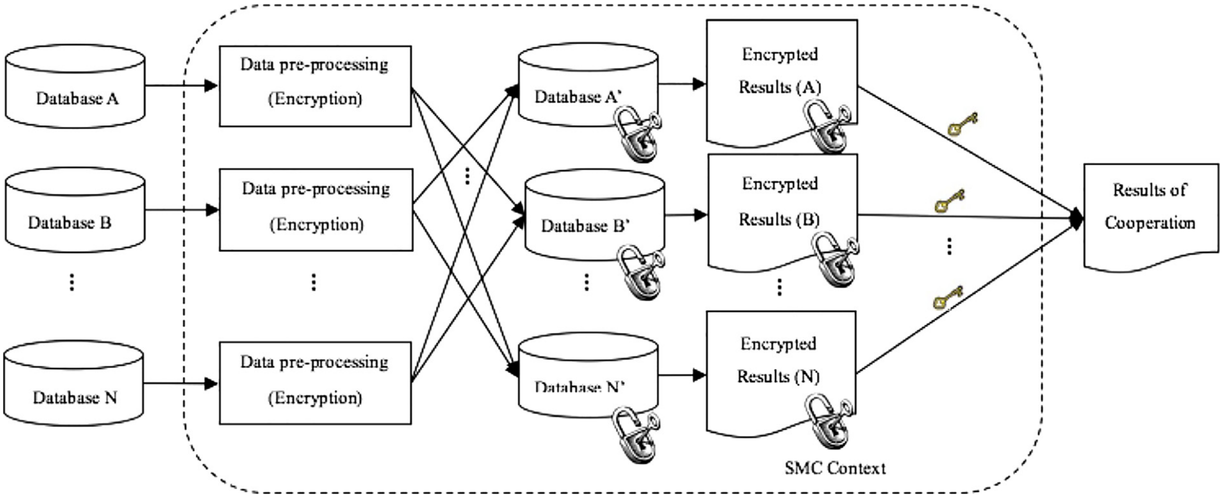

Fig. 1. The overview of processing private data without a trusted third party.

significantly hinder collaborative decision making and optimal supply chain arrangements.

Similar challenges exist in other areas, such as health care centers [10], credit and loan evaluation processes [11], government organizations [12], and database marketing and Web usage analysis companies [13], which use sensitive data from distributed databases held by different parties to make predictions and decisions. Despite the well-known benefits, many organizations are averse to sharing individuals' private information.

A commonly adopted strategy to address problems related to private information sharing is to assume the trustworthiness of the participants, or to assume the existence of a trusted third party to facilitate data exchange. However, in reality there cannot be a completely trusted third party where the pursuit of commercial interests is concerned. Therefore, in this study, we propose an encryption protocol by integrating Secure Multi-Party Computation (SMC) with the Karmarkar algorithm for sharing and calculating private information in the context of cross-organizational collaboration. We also address the issue of computation speed for processing big data.

1.1. Problem statement

In this study, we introduce the SMC to address the above-mentioned problems. As shown in Fig. 1, the information needed for collaboration often resides in different data holders' individual databases. Moreover, such multi-party collaboration may be characterised by a least trust level due to the existence of direct competition between the parties. Nevertheless, all parties recognize the benefits brought by such a collaboration. Under the precondition of preserving privacy, all parties in the collaboration promise to provide their private data to achieve mutual benefit and meanwhile plan to minimize costs in a context without a trusted third party.

1.2. Our contribution

Although the traditional SMC might be effective in handling small data sets, they are often inefficient for large data sets that are associated with big data. Even though a lot of effort has been spent on addressing this weaknesses, efficient and effective solutions of multi-party computations (MPC) based on large private inputs have yet to be developed. Moreover, regardless of computational efficiency, it is impossible to directly apply the theoretical MPC work for small datasets to form secure protocols with large datasets in distributed information analysis.

In order to address the above issues, we attempt to identify potential solutions so as to balance the practicality and efficiency issues in this study. Specifically, we introduce the revised Karmarkar algorithm to deal with privacy-preserving distributed LP for MPC and two-party computation (TPC) in the scenario of mutual distrust and semi-honest participants. Our contributions can be summarized as follows: (1) both collaborative effectiveness and efficiency can be achieved by applying the revised Karmarkar algorithm in the context of SMC, as confirmed by our simulation results; (2) The proposed protocols are suitable for large data sets, as validated by our stimulations; (3) The proposed protocols are applicable to both collaborative optimization and protecting private information.

Following this introduction, the rest of this paper is structured as follows. Section 2 explains the preliminaries for our approach, focusing in particular on the reasons why we chose the Karmarkar algorithm for SMC. Section 3 defines the research problems, followed by the secure protocol with security proof and complexity analysis in multi-party collaboration. Then we detail the processes for two-party collaboration in Section 4. Finally, we experimentally validate the protocol and analyze the result in Section 5 and conclude the paper with implications and future work in Section 6.

2. The model

2.1. Original Secure Multi-Party Computation

A number of scholars [e.g., [4,14]] have designed different information security mechanisms. Specifically, Yao [15] put forward a constant-round protocol for Secure Two-Party Computation (STC) in the presence of semi-honest adversaries in the context of auctions and bidding. His work has received wide attention in the field of information security. Specifically, the semi-honest situation is defined as: "participants are expected to follow protocol specifications [16], but they record intermediate values observed during the protocol which can be employed to compromise security" [17]. Thus the concept of STC was generalized to SMC [18], which has now became a subfield of cryptography "with the goal to create methods for parties to jointly compute a function over their inputs, and keeping these inputs private" [19].

In order to specify the security protocols and better apply the concept of SMC in reality, the efficient SMC frameworks were proposed [20]. Among them, the invertible-matrix and commodity-based approaches [21] were offered to modify the basic SMC model, subsequently suggesting a better balance of efficiency