Information Sciences 506 (2020) 325–345

Contents lists available at ScienceDirect

Information Sciences

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

PGAS: Privacy-preserving graph encryption for accurate constrained shortest distance queries

Can Zhang[a], Liehuang Zhu[a,*], Chang Xu[a,*], Kashif Sharif[a], Chuan Zhang[a], Ximeng Liu[b,c,d]

[a] School of Computer Science & Technology, Beijing Institute of Technology, Beijing, China
[b] College of Mathematics and Computer Science, Fuzhou University, Fuzhou, China
[c] Fujian Provincial Key Laboratory of Information Security of Network Systems, Fuzhou, China
[d] School of Information Systems, Singapore Management University, Singapore

ARTICLE INFO

Article history:
Received 6 December 2018
Revised 23 July 2019
Accepted 24 July 2019
Available online 5 August 2019

Keywords:
Cloud computing
Graph encryption
Constrained shortest distance query
Outsourced computing

ABSTRACT

The constrained shortest distance (CSD) query is used to determine the shortest distance between two vertices of a graph while ensuring that the total cost remains lower than a given threshold. The virtually unlimited storage and processing capabilities of cloud computing have enabled the graph owners to outsource their graph data to cloud servers. However, it may introduce privacy challenges that are difficult to address. In recent years, some relevant schemes that support the shortest distance query on the encrypted graph have been proposed. Unfortunately, some of them have unacceptable query accuracy, and some of them leak sensitive information that jeopardizes the graph privacy. In this work, we propose **P**rivacy-preserving **G**raph encryption for **A**ccurate constrained **S**hortest distance queries, called **PGAS**. This solution is capable of providing accurate CSD queries and ensures the privacy of the graph data. Besides, we also propose a secure integer comparison protocol and a secure minimum value protocol that realize two kinds of operations on encrypted integers. We provide theoretical security analysis to prove that PGAS achieves *CQA-2 Security* with less privacy leakage. In addition, the performance analysis and experimental evaluation based on real-world dataset show that PGAS achieves 100% accuracy with acceptable efficiency.

© 2019 Elsevier Inc. All rights reserved.

1. Introduction

Graphs and graph data have been used in many fields of sciences and engineering for a long time. With the advancements in information technology, it has not only found its use in computer sciences but has enabled digitization of graph data for other domains. These domains include large scale Internet topologies, online social networks, biometric networks, communication systems, road networks, and so on. Similarly, with its widespread usage, a handful of tools have also been proposed in order to analyze and process massive graphs (e.g., GraphLab [23], TurboGraph++ [16] and GraphBase).

The shortest distance query has been considered as one of the most fundamental operations of graphs and has a wide range of applications. In online social networks, assume that `Alice` wants to meet a stranger `Bob`, the shortest distance query can return the minimum number of intermediate nodes between `Alice` and `Bob`. Compared to the shortest distance

* Corresponding author.
E-mail addresses: liehuangz@bit.edu.cn (L. Zhu), xuchang@bit.edu.cn (C. Xu).

https://doi.org/10.1016/j.ins.2019.07.082
0020-0255/© 2019 Elsevier Inc. All rights reserved.

query, constrained shortest distance (CSD) query is a specialized kind that considers both the shortest distance as well as cost conditions. For example, in road networks, CSD queries can be used if a user intends to find the shortest distance from the source s to the destination t while maintaining the total time cost below the threshold θ.

The graph owners can benefit from cloud storage systems by outsourcing the massive graph data to third-party servers. This will reduce the maintenance and management costs for such organizations. However, this increases the risk of potential leakage of data, which may compromise the user's privacy. To tackle this privacy challenge, graph owners can encrypt their graph data before outsourcing it to the cloud server, however, simply encrypting the graph data results in loss of querying abilities of graphs. Taking the CSD query as an example, some methods have been proposed to solve the approximate or exact (accurate) CSD query problems on plain graphs [11,32,33,35]. Unfortunately, these schemes cannot be directly used on encrypted graphs.

In order to alleviate the privacy concerns, some methods have been presented in the literature to protect access privacy [38,44], query privacy [39], identity privacy [13], data privacy [42,43], and location privacy [14] in cloud computing environments. Chase et al. [5] first proposed the concept of graph encryption to protect graph data privacy and query privacy. Using such encryption methods, graph owners can outsource the encrypted graph data to a semi-honest cloud server without losing the querying abilities. A series of graph encryption schemes that support the shortest distance query have also been proposed in [24,30]. These schemes make use of cryptographic primitives (e.g., Homomorphic Encryption, Pseudo-Random Function, and Order Revealing Encryption) to encrypt the graph itself or the corresponding pre-generated index. Unfortunately, some of the existing schemes do not support constraint filtering during the shortest distance query processes, which means that they do not support the CSD query. Moreover, some of them only return an approximate query result, and some of them even have unacceptable leakage that jeopardizes the graph privacy.

In light of these shortcomings in existing schemes, we propose a privacy-preserving graph encryption scheme that supports accurate constrained shortest distance (ACSD) queries. Our scheme makes use of the Paillier Cryptosystem with Threshold Decryption to encrypt the distance and cost values in a graph's Two-Hop Cover Label. Our scheme also separates the storage and computation of outsourced data which achieves advanced privacy protection. We also propose a privacy-preserving security integer comparison protocol and a secure minimum value protocol. Hence, the scheme can return ACSD query results with acceptable leakage.

To the best of our knowledge, this is the first graph encryption scheme that supports ACSD queries (i.e., it returns accurate CSD query results) with privacy protection.

Following are the major contributions of this work:

- We propose the complete system architecture of the graph encryption scheme that supports ACSD queries. Our architecture separates the storage and computation of outsourced data, which realizes advanced privacy protection.
- We present PGAS, the first graph encryption scheme that supports ACSD queries on encrypted graph data. PGAS uses the Constraint Filtering algorithm to filter the cost values. Besides, PGAS can return accurate query results to the user.
- We propose two novel protocols: The *Secure Integer Comparison* (*SIC*) protocol compares two encrypted integers, and the *Secure Minimum value* (*SMin*) protocol finds the minimum value of some encrypted integers. Both protocols directly operate the ciphertexts, so they do not reveal any information about plaintexts. In addition, these protocols can be used not only in our proposed scheme but also in other relevant application scenarios.
- We also present a strict security analysis of PGAS to prove that it can achieve *CQA2-Security*. We also make a throughout the theoretical analysis and comprehensive experimental evaluation based on real-world datasets to show that our proposed scheme has acceptable efficiency and achieves 100% accuracy.

The rest of this paper is organized as follows. In Section 2, we describe related works. In Section 3, we make a brief introduction of the Two-Hop Cover Label and the Paillier Cryptosystem with Threshold Decryption and define the graph encryption scheme that supports ACSD queries. The formalized scenario and security model are defined in Section 4. Detailed descriptions of PGAS are presented in Section 5, and in Section 6 we present two kinds of secure outsourced integer computation protocols *SIC* and *SMin*. Security analysis is given in Section 7. Performance analysis and experimental evaluation are presented in Section 8. Finally, Section 9 concludes this paper.

2. Related works

2.1. Constrained shortest distance query

CSD query is a special kind of shortest distance query on graphs. It has received much attention to its cost condition capabilities. Hansen [11] proposed a scheme to find the exact constrained shortest path based on enhanced Dijkstra's algorithm. Tsaggouris et al. [33] provided an optimized method to find the approximate constrained shortest path with improved efficiency. Both of these schemes are not practical for processing large graphs due to the high computation costs. In order to improve the efficiency, some schemes use a pre-generated index to speed up the query process. Storandt [32] proposed a method to find the exact constrained shortest path with an index, but it still requires significant query processing.

In recent years, a series of efficient schemes have been proposed to solve constrained shortest path problems. Wang et al. [35] presented a practical solution for index-based approximate constrained shortest path querying for large road networks. Bode et al. [2] provided a labeling algorithm to solve the shortest path problem under resource constraints with (k,2)-loop

Download English Version:

https://daneshyari.com/en/article/13429086

Download Persian Version:

https://daneshyari.com/article/13429086

Daneshyari.com