Information Sciences 280 (2014) 205–217

Contents lists available at ScienceDirect

Information Sciences

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

Achieving security, robust cheating resistance, and high-efficiency for outsourcing large matrix multiplication computation to a malicious cloud

Xinyu Lei [a,*], Xiaofeng Liao [a], Tingwen Huang [b], Feno Heriniaina [a]

[a] The State Key Lab. of Power Transmission Equipment & System Security and New Technology, College of Computer Science, Chongqing University, Chongqing, China
[b] Texas A&M University at Qatar, P.O. Box 23874, Doha, Qatar

ARTICLE INFO

Article history:
Received 22 June 2013
Received in revised form 6 May 2014
Accepted 10 May 2014
Available online 16 May 2014

Keywords:
Cloud computing
Matrix multiplication
Secure outsourcing
Monte Carlo verification

ABSTRACT

Computation outsourcing to the cloud has become a popular application in the age of cloud computing. This computing paradigm brings in some new security concerns and challenges, such as input/output privacy and result verifiability. Given that matrix multiplication computation (MMC) is a ubiquitous scientific and engineering computational task, we are motivated to design a protocol to enable secure, robust cheating resistant, and efficient outsourcing of MMC to a malicious cloud in this paper. The main idea to protect the privacy is employing some transformations on the original MMC problem to get an encrypted MMC problem which is sent to the cloud; and then transforming the result returned from the cloud to get the correct result to the original MMC problem. Next, a randomized Monte Carlo verification algorithm with one-sided error is introduced to successfully handle result verification. We analytically show that the proposed protocol is correct, secure, and robust cheating resistant. Extensive theoretical analysis and experimental evaluation also show its high-efficiency and immediate practicability. Finally, comparisons between the proposed protocol and the previous protocols are given to demonstrate the improvements of the proposed protocol.

© 2014 Elsevier Inc. All rights reserved.

1. Introduction

With the emergence of the cloud computing paradigm in scientific and business applications, it has become increasingly important to provide service-oriented computing in third-party data management settings [24,23]. Cloud computing is capable of providing massive computing resources to clients as services while hiding implementation details from clients [1,32]. With this paradigm, the resource-constrained clients can off-load their intensive computational tasks to clouds, which are equipped with massive computational resources. In contrast to setting up and maintaining their own infrastructures, the clients can economically share the massive computational power, storage, and even some softwares of the cloud servers.

1.1. Challenges

Although it is quite promising, outsourcing computational problem to the commercial public inevitably brings in new security concerns and challenges [6,21,22,35]. The first challenge is the client's input/output data privacy. The outsourced

* Corresponding author. Tel.: +86 13658371220.
E-mail address: xy-lei@qq.com (X. Lei).

http://dx.doi.org/10.1016/j.ins.2014.05.014
0020-0255/© 2014 Elsevier Inc. All rights reserved.

computational problems and their results often contain sensitive information, such as the business financial records, VIP customers lists, engineering data, or proprietary asset data, etc. To hide these information from the cloud, clients need to encrypt their data before outsourcing and decrypt the returned result from the cloud after outsourcing. The second challenge is the verification of the result returned by the cloud. A cloud server might not always provide the accurate result of a given computational task. As an example of intentional reasons, for the outsourced computational intensive tasks, there are strong financial incentives for the cloud to be lazy and just return incorrect answers to the client if such answers require less work and are unlikely to be detected by the client. Besides, some accidental reasons such as possible software bugs or hardware failures may also result in wrong computational results. Consequently, the outsourcing protocol must be designed in such a way that it is able to detect whether the returned result is correct. The third challenge is efficiency. On one hand, a key requirement is that the amount of local work performed by the client must be substantially cheaper than performing the original computational problem on its own. Otherwise, it does not make sense for the client to resort to the cloud. On the other hand, it is also desirable to maintain the amount of work performed by the cloud as close as possible to that needed to compute the original problem by the client itself. Otherwise, the cloud may be unable to complete the task in a reasonable amount of time, or the cost of the cloud may become prohibitive. To summarize, a protocol for computation outsourcing should satisfy the following for aspects: correctness, security, verifiability and efficiency.

1.2. Motivations

Matrix multiplication computation (MMC) is a basic computational problem in scientific and engineering fields and has a number of applications. This can be well illustrated by the following examples. MMC is frequently used in statistics theory. Take a typical linear regression model $\mathbf{y} = \mathbf{X}\beta$ as an example, the least squared error method yields an solution for β by computing $\beta = (\mathbf{X}^T\mathbf{X})^{-1}\mathbf{X}^T\mathbf{y}$ [29]. Besides, MMC plays an important role in linear algebra and matrix theory [26]. For instance, the linear discrete dynamical systems are best studied in a matrix formulation $\mathbf{x}_{n+1} = \mathbf{A}\mathbf{x}_n$, where the solution is $\mathbf{x}_n = \mathbf{A}^n\mathbf{x}_0$. The computation of $\mathbf{A}^n$ allows us to obtain this solution. Moreover, MMC is well rooted in many other scientific and engineering fields including image encryption [31,38], 3D graphics simulations [13], discriminant analysis [36,27], sliding mode analysis [16,4], to just list a few. In short, MMC is widely needed for a variety of potential clients. When the restricted computational resources are possessed by these clients and MMC deals with large matrices, an economical solution is to outsource MMC to a powerful cloud. Even if the data is in a moderate scale, for clients as battery-limited mobile phones, portable devices, or embedded smart cards, secure outsourcing of MMC is preferred. Consequently, we are motivated to design a protocol that enables clients to securely, verifiably, and efficiently outsource MMC to a cloud.

1.3. Contributions

We regard our main contributions as fourfold:

1. We identify a common scientific and engineering computational task, i.e., matrix multiplication computation outsourcing, and then design a protocol to fulfill it.
2. We show that the proposed protocol can simultaneously achieve goals of correctness, security, robust cheating resistance, and efficiency.
3. By introducing Monte Carlo verification algorithm, the problem of result verification is well addressed. Additionally, the superiority of Monte Carlo verification algorithm in designing inexpensive result verification algorithm for secure outsourcing is well demonstrated.
4. We show by theoretical analysis and experimental evaluation that the proposed protocol is highly efficient, and therefore, it can be deployed in practical applications immediately.

1.4. Organization

The remainder of this paper proceeds as follows. Section 2 introduces some essential preliminaries. In Section 3, we describe the proposed protocol with detailed techniques. Sections 4 and 5 give some related analysis and performance evaluation, followed by Section 6 which overviews the related work. Finally, some conclusions are drawn in Section 7.

2. Preliminaries

2.1. System model, threat model, design goals, and framework

2.1.1. System model

We consider the secure MMC outsourcing system model, as illustrated in Fig. 1. A client with low computational power intends to outsource the multiplication computation of matrices $\mathbf{X}$ and $\mathbf{Y}$, denoted as $\Phi = (\mathbf{X}, \mathbf{Y})$, to a cloud service provider, who has massive computational power and special softwares. In order to protect input privacy, the client encrypts the original MMC problem Φ using a secret key K to get a new computational problem, written as Φ_K. Later, the encrypted

Download English Version:

https://daneshyari.com/en/article/391639

Download Persian Version:

https://daneshyari.com/article/391639

Daneshyari.com