Indonesian Journal of Electrical Engineering and Computer Science
Vol. 16, No. 2, November 2019, pp. 1065∼1069
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v16i2.pp1065-1069

Privacy preserving outsourcing algorithm for two-point linear boundary value problems

Nedal M. Mohammed[1], Laman R. Sultan[2], Santosh S. Lomte[3]
[1,3]Department of Computer Science , Dr. Babasaheb Ambedkar Marathwada University , Aurangabad, India
[2]Department of Power Mechanics, Basra Technical Institute, Southern Technical University, Al-Basrah, Iraq

Article Info

Article history:

Received Jan 25, 2019
Revised Apr 15, 2019
Accepted May 3, 2019

Keywords:

Cloud computing
Secure computation outsourcing
Verifiable computing
Secure and privacy BVP.

ABSTRACT

One of a powerful application in the age of cloud computing is the outsourcing of scientific computations to cloud computing which makes cloud computing a very powerful computing paradigm, where the customers with limited computing resource and storage devices can outsource the sophisticated computation workloads into powerful service providers. One of scientific computations problem is Two-Point Boundary Value Problems (BVP) is a basic engineering and scientific problem, which has application in various domains. In this paper, we propose a privacy-preserving, verifiable and efficient algorithm for two-point BVP in outsourcing paradigm. We implement the proposed schema on the customer side laptop and using AWS compute domain elastic compute cloud (EC2) for the cloud side.

Corresponding Author:

Nedal M. Mohammed,
Department of Computer Science,
Taiz University, Taiz, Yemen.
Email: dr.nedal.mohammed@gmail.com

1. INTRODUCTION

The powerful advantages of cloud computing is called outsourcing, where the customers with limited computing resource and storage devices can outsource the sophisticated computation workloads into powerful service providers. Despite the tremendous benefits, there are many challenges and security concerns because the cloud server and customer are not in the same trusted domain, to avoid these problems [1, 2, 3, 10]. First, to combat the security concern is applying encryption techniques to customer's sensitive information before outsourcing to the cloud but still, there is a challenge how makes the task of computation over encrypted data [2, 4, 8]. Second, no guarantee from the cloud on the quality of the computed data and results. Focusing on scientific and engineering applications problems we notice that the differential equations problems (Boundary value problems and initial value problems). The BVP & IVP frequently appear in various fields and has a number of applications, but solving these large-scale BVP & IVP problems is usually computationally so expensive [5, 7, 9, 11]. The computers with limited computing resource and storage devices are facing the challenge of solving large-scale BVP & IVP. To address this challenge (solving large-scale BVP & IVP), an alternative option is outsourcing to cloud computing.

This work, focusing on secure outsourcing BVP. We are proposing secure, efficient and verifiable scheme to offload large-scale BVP computation to cloud side. This paper is organized as follows Section 2. describes our proposed system model to secure outsourcing the BVP problem. In Section 3. outsourcing algorithm of two-point BVP. In Section 4. security analysis of proposed algorithm. In Section 5. we provide experimental result analysis for proposed schema. At last the work conclusion is presented in section 6.

2. SYSTEM MODEL

We consider an asymmetric architecture involved two parties. On the first side, there is a resource-constrained customer who has the BVP problem to solve However, due to limited computing resources the customer cannot do this computation to solve the problem locally. On second side, (S) cloud with computationally powerful devices and huge storage facilities, but cannot be trusted with the sensitive information. Then to avoid security problems the procedure goes as shown in Figure 1.

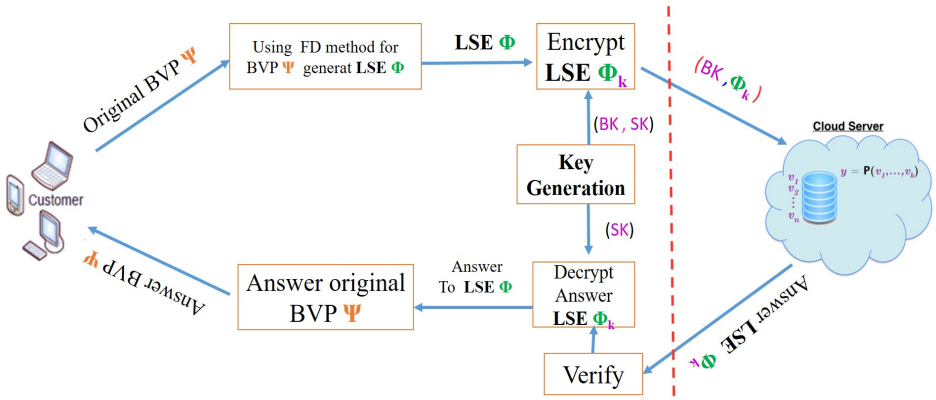

Figure 1. System model of secure outsourcing of BVP problem.

We consider the procedure is gowing as follow the customer C outsource an BVP Ψ computation task $\Psi : D \rightarrow M$ to a cloud server S. However, S is not fully trusted by C either semi-honest or malicious. So to protect the input privacy, the C transfers the original BVP Ψ to linear system equation (LSE) Φ then encrypts Φ into an encrypted Φ_k with a secret Key K then. Then Φ_k is outscrced from the C to the S. The S runs optimization algorithm to solve Φ_k when receiving the encrypted BVP problem Φ_k. After getting the result, the C verifies whether the solution returned is correct or not in encryption domain. If the result can not pass through verification, C requires the cloud to compute it again. Otherwise, the customer decrypting the correct result to get the solution to the BVP Ψ.

3. OUTSOURCING ALGORITHM OF TWO-POINT BOUNDARY VALUE PROBLEMS

In this section, we propose algorithm for securely outsourcing large-scale system of finite difference method to find the solution of linear boundary value problems. To achieve goals of our work, we design the following sub-algorithms.

3.1. Using Finite Difference Method

Two-Point linear boundary value problems formulated as[6, 5, 9]:

$$\begin{aligned} &u'' = p(t)u' + q(t)u + r(t), \quad t \in [a, b], \\ &u(a) = \alpha, u(b) = \beta. \end{aligned} \tag{1}$$

The problem for securely outsourcing large-scale Linear BVP with Finite Differences can be formulated as follows: The client C seeks for the solution to a large-scale Linear Boundary Value Problems $A_h y_h = b_h$, where $A_h \in R^{N \times N}$ is given matrix in the form [8, 9]

$$A_h = \begin{pmatrix} 2 & -1 & 0 & \dots & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & \dots & 0 & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & \dots & 0 & 2 & 1 & 0 \end{pmatrix}$$

and $b_h \in R^N$ is a vector of the form

$$b_h = \begin{pmatrix} -r(t_1) + \dfrac{\alpha}{h^2} \\ -r(t_i), i = 2, 3, \ldots, N-1 \\ -r(t_N) + \dfrac{\beta}{h^2} \end{pmatrix}$$

3.2. Key Generation Algorithm.

In key generation algorithm, client firstly picks a random disguising coefficient vector $r \in R^n$ and $M, N \in R^{n \times n}$, two random sparse matrices as below.

$$\begin{aligned} M(i;f) &= m_i \delta_{\Psi m(i)} \qquad f1 \leq i; f \leq m; \\ N(i;f) &= n_i \delta_{\Psi n(i)} \qquad f1 \leq i; f \leq n; \\ r(i) &= r_i \qquad 1 \leq i \leq n. \end{aligned} \tag{2}$$

Here $m_i; n_i; r_i$ are all randomly generated from the spaceΩ and Ψ_m, Ψ_n are two different bijection functions. These two key matrices and one vector constitute the key which can be written as $K(M, N, r)$ and must be kept secret by client.

3.3. Outsourcing Algorithm

Due to the lack of computing resources, C could be infeasible to carry out such expensive computation as $O(n^\rho)$ for $2 < \rho \leq 3$ locally. Therefore, client will outsource the computation workloads to cloud server in a pay-per-use manner [11].

Client chooses $M, N \in R^{nn}$ two random sparse matrices which generate from 3.2. to hide A_h then computes $K = MA_hN$. So that the input of problem generation (ProbGen) algorithm is a coefficient matrix $A_h u_h A \in R^{n \times n}$ and a coefficient vector $b_h \in R^n$.

From above transformation the original matrix of finite difference method of BVP can be rewritten as $A(x + r)_h = c$. Then, C computes $K = MAN$and $d = Mc$. Without loss of generality, we denote $u = N^{-1}(x+r)$, where N^{-1} is the inverse of matrix N. Note that in our algorithm, no party needs to compute $N1$. It appears here only for representing the form of u. In fact, if N^{-1} had to be computed, the algorithm would no longer be efficient as the time and computational complexities incurred by computing N^{-1} would be very undesirable. Note that $Ku_h = MA_hN \cdot pN^{-1}(u_h + r) = MA(u_h + r) = Mc = d$, then outsource this K, d to the cloud and get th solution as a coefficient vector u_h such that $K_h u_h = d_h$. Using the random disguising technique, we can prove the privacy of proposed outsourcing schema for A_h, b_h and the solution x. Besides, The proposed schema only requires one round interaction between cloud and server and does not require any special encryption techniques, so the complexity to compute K is $O(n^2)$.

4. SECURITY ANALYSIS

Theorem 1: *In the fully malicious model, the algorithms (C, S) are privacy for A_h, b_h, and u_h.*

Proof. We first prove the privacy for input b_h and output u_h of BVP. Note that the adversaryA_h can only know K and d throughout the whole algorithm. Besides, we have $b_h = M^{-1}d - Ar$, and $u_h = Nx - r$. Since r is a random blinding coefficient vector in R^n, both b and u_h are blinded by r in the sense of indistinguishability. We then prove the privacy for input A_h. Let $M = (m_{ij}), N = (n_{ij}), M' = (m_{ij})$, and $N' = (n'_{ij})$ be four random nonsingular sparse matrices generated by C. Given two nonsingular dense matrices $A = (aij)$ and $A' = (a'_{ij})$ which are chosen by the adversary A_h, C computes $K = MA_hN = (k_{ij})$ and $K' = M'A_h{}'N' = (k'_{ij})$, where

$$k_{ij} = \sum_{i=1}^{n} \sum_{j=1}^{n} m_{if} \cdot a_{kf} \cdot n_{if}$$

and

$$t'_{ij} = \sum_{i=1}^{n}\sum_{j=1}^{n} m'_{if} \cdot a'_{fi} \cdot n'_{ij}$$

Note that the numerical value and position of all non-zero elements of four matrices M, N, M' and N' are randomly chosen by C, thus k_{ij} and k'_{ij} are computationally indistinguishable. As a result, the advantage of A_h to distinguish between K and K' is negligible.

Theorem 2: *In the fully malicious model, the algorithms (C, S) are an $O(\frac{1}{n})$ efficient implementation of schema.*

Proof. In the proposed algorithm, C needs to perform four matrix-vector multiplication (we omit the vector-addition operations), which takes $O(n^2)$ computations. Besides, C also needs to compute $K = MAN$, which also takes $O(n^2)$ computations. Thus, the efficient implementation of our algorithm (C, S) are an $O(\frac{1}{n})$.

5. EXPERIMENTAL RESULT ANALYSIS

The experimental results are the average of multiple trials. We design numerical experiments to evaluate the efficiency of the mechanism. We implemented it using Matlab (2013a), with the system configuration is "$CPU \quad Intel^{®} \quad Core^{™} i3(CPUs)$ ~$1.8GHZ4GB \quad Ram$" on a laptop and Amazon Elastic Compute Cloud (EC2) cluster. The test benchmark for randomly generated sparse matrices only focuses on the large-scale problems where n ranges from $5,000$ to $20,000$, as Table 1.

Table 1. Performance of the proposed scheme

	Problem Size	KeyGen Algorithm	ProbGen Algorithm	Verify Algorithm	Solve Algorithm	Client Cost Time
1	$n = 5000$	10.15	116.88	6.13	10.54	133.03
2	$n = 10000$	19.20	231.23	10.89	14.02	261.32
3	$n = 15000$	23.13	347.72	20.54	17.43	391.39
4	$n = 20000$	33.97	580.73	27.85	18.56	642.55

To measure the efficiency of our proposed mechanism, we simulated all four phases (i.e., KeyGen, ProbGen, Verify and solve). The corresponding time costs for different size of problems are shown in Figure 2.

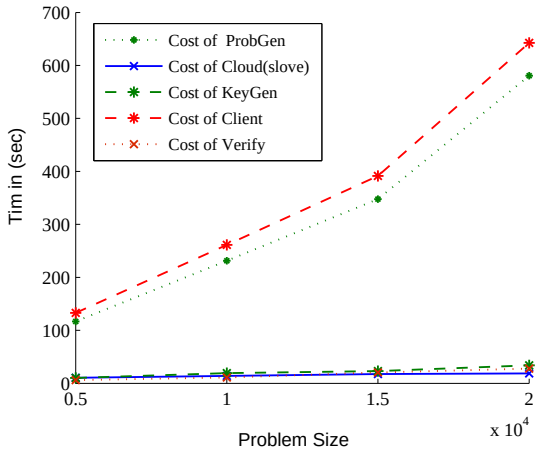

Figure 2. Time cost for each phase of secure outsourcing BVP algorithm.

6. CONCLUSION

In this paper, we proposed a new secure, efficient algorithm for securely outsourcing of large-scale finite difference method to find the solution of linear BVP computation using cloud computing. We implement schema on the customer side laptop and using AWS compute domain elastic compute cloud (EC2) for the cloud side. We find that the proposed schema is suitable to approximate solutions to differential equations (BVP) problem and only requires $O(n^2)$ computational overhead even in the fully malicious model.

REFERENCES

[1] C. Hu, A. Alhothaily, A. Alrawais, X. Cheng, C. Sturtivant and H. Liu, "A secure and verifiable outsourcing scheme for matrix inverse computation," *IEEE INFOCOM'17 (Atlanta, GA, USA)*, Vol. 4, pp. 2304–2312, 2017.

[2] N. M. Mohammed and S. S. Lomte, "Recent advances on secure computations outsourcing in cloud computing," *Asian Journal of Mathematics and Computer Research*, Vol. 24, pp.192–205, 2017.

[3] K. Zhou and J. Ren, "CASO: Cost-Aware Secure Outsourcing of General Computational Problems," *IEEE Transactions on Services Computing*, 2018.

[4] W. Shen, Y. Bo, C. Xianghui, C. Yu and S. Xuemin, "A distributed secure outsourcing scheme for solving linear algebraic equations in ad hoc clouds," *IEEE Transactions on Cloud Computing*, Vol. 4, 2017.

[5] H. C. Saxena, "Finite-Differences and Numerical Analysis, Thirteen Revised Edition," *Published by S. Chand& Company Ltd. New Delhi*, 1997.

[6] U. Ascher, R. Mattheij and R. Russell, "Numerical Solution of Boundary Value Problems for Ordinary Differential Equations," *Prentice-Hall*, 1988.

[7] N. M. Mohammed and S. S. Lomte, "Secure Computations Outsourcing of Mathematical Optimization and Linear Algebra Tasks: Survey," *International Journal for Research in Engineering Application & Management*, pp. 6–11, 2019.

[8] A. George and J. Liu, "Computer Solution of Large Sparse Positive-definite Systems," *Prentice-Hall*, 1981.

[9] D. M. Young, "Iterative Solution of Large Linear Systems," *Academic Press*, 1971.

[10] N. M. Mohammed and S. S. Lomte, "Secure and Efficient Outsourcing of Large Scale Linear Fractional Programming," *International Conference on Computing in Engineering and Technology(ICCET)*, 2019, To Appear.

[11] S. Salinas, C. Luo, X. Chen, W. Liao and P. Li, "Efficient Secure Outsourcing of Large-scale Sparse Linear Systems of Equations," *IEEE Transactions on Big Data*, 2017. DOI 10.1109/TBDATA.2017.2679760,