INTERNATIONAL JOURNAL OF COMPUTATIONAL MATHEMATICAL IDEAS [IJCMI] ISSN: 0974-8652
WWW.IJCMI.COM/VOL 15-APRIL-MAY -2017

A Distributed Secure Improved Linear Programing based Performance Computation out Sourcing in Cloud Computing

VENKATESH Ch [1] Mr. KALLAM GOPALA REDDY [2]
RAMACHANDRA COLLEGE OF ENGINEERING
Published in Volume 15, Issue 1 April – May : 2017,PageNo: 71575 -71580

Abstract

We investigate the outsourcing of numerical and scientific computations using the following framework: A customer who needs computations done but lacks the computational resources (computing power, appropriate software, or programming expertise) to do these locally would like to use an external agent to perform these computations. This currently arises in many practical situations, including the financial services and petroleum services industries. The outsourcing is secure if it is done without revealing to the external agent either the actual data or the actual answer to the computations. The general idea is for the customer to do some carefully designed local preprocessing (disguising) of the problem and/or data before sending it to the agent, and also some local post processing of the answer returned to extract the true answer. The disguise process should be as lightweight as possible, e.g., take time proportional to the size of the input and answer. The disguise preprocessing that the customer performs locally to "hide" the real computation can change the numerical properties of the computation so that numerical stability must be considered as well as security and computational performance. We present a framework for disguising scientific computations and discuss their costs, numerical properties, and levels of security. We show that no single disguise technique is suitable for a broad range of scientific computations but there is an array of disguise techniques available so that almost any scientific computation could be disguised at a reasonable cost and with very high levels of security. These disguise techniques can be embedded in a very high level, easy-to-use system (problem solving environment) that hides their complexity.

Keywords: Linear Programming, Hybrid Cloud Computing, Virtual Networks, Security, Encryption and Decryption

Introduction:

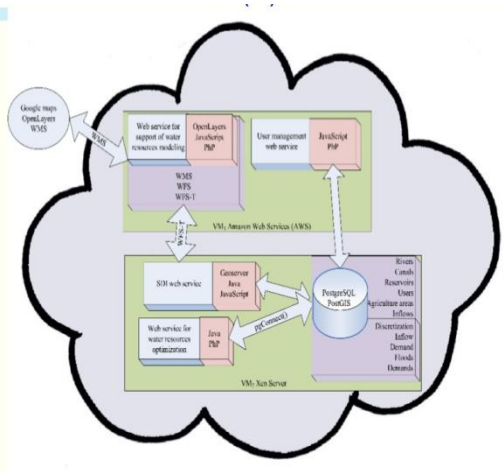
Suppose that you want to delegate the ability to *process* your data, without giving away *access* to it. We show that this separation is possible: we describe a "fully homomorphic" encryption scheme that keeps data private, but that allows a worker that *does not have the secret decryption key* to compute any (still encrypted) result of the data, even when the function of the data is very complex. In short, a third party can perform complicated processing of data without being able to see it. Among other things, this helps make cloud computing compatible with privacy

Cloud computing enables an economically promising paradigm of computation outsourcing. However, how to protect customers confidential data processed and generated during the computation is becoming the major security concern. Focusing on engineering computing and optimization tasks, this paper investigates secure outsourcing of widely applicable linear programming (LP) computations. Our mechanism design explicitly decomposes LP computation outsourcing into public LP solvers running on the cloud and private LP parameters owned by the customer. The resulting flexibility allows us to explore appropriate security/efficiency tradeoff via higher-level abstraction of LP computation than the general circuit representation. Specifically, by formulating private LP problem as a set of matrices/vectors, we develop efficient privacy-preserving problem transformation techniques, which allow customers to transform the original LP into some random one while protecting sensitive input/output information. To validate the computation result, we further explore the fundamental duality theorem of LP and derive the necessary and sufficient conditions that correct results must satisfy. Such result verification mechanism is very efficient and incurs close-to-zero additional cost on both cloud server and customers. Extensive security analysis and experiment results show the immediate practicability of our mechanism design.However, security is the major concern that prevents the wide adoption of computation

outsourcing in the cloud, especially when end-user's confidential data are processed and produced during the computation. Thus, secure outsourcing mechanisms are in great need to not only protect sensitive information by enabling computations with encrypted data, but also protect customers from malicious behaviors by validating the computation result. Such a mechanism of general secure computation outsourcing was recently shown to be feasible in theory, but to design mechanisms that are practically efficient remains a very challenging problem. Focusing on engineering computing and optimization tasks, this paper investigates secure outsourcing of widely applicable linear programming (LP) computations. In order to achieve practical efficiency, our mechanism design explicitly decomposes the LP computation outsourcing into public LP solvers running on the cloud and private LP parameters owned by the customer. The resulting flexibility allows us to explore appropriate security/efficiency tradeoff via higher-level abstraction of LP computations than the general circuit representation. In particular, by formulating private data owned by the customer for LP problem as a set of matrices and vectors, we are able to develop a set of efficient privacy-preserving problem transformation techniques, which allow customers to transform original LP problem into some random one while protecting sensitive input/output information. To validate the computation result, we further explore the fundamental duality theorem of LP computation and derive the necessary and sufficient conditions that correct result must satisfy. Such result verification mechanism is extremely efficient and incurs close-to-zero additional cost on both cloud server and customers. Extensive security analysis and experiment results show the immediate practicability of our mechanism design.

Architecture:

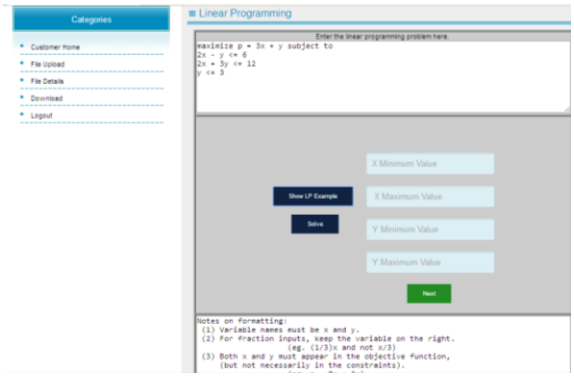
INTERNATIONAL JOURNAL OF COMPUTATIONAL MATHEMATICAL IDEAS [IJCMI] ISSN: 0974-8652
WWW.IJCMI.COM/VOL 15-APRIL-MAY -2017



Linear Programming Methodology:

Secure LP outsourcing in cloud can be represented by decomposing LP computation into public LP solvers running on the cloud and private data owned by the customer. Because different decompositions of LP usually lead to different trade-offs among efficiency and security guarantees, how to choose the right one that is most suitable for our design goal is thus of critical importance. To systematically study the difference, we organize the different decompositions into a hierarchy which ensembles the usual way that a computation is specified: a computation at a higher abstraction level is made up from the computations at lower abstraction levels. At higher abstraction levels, more information about the computations becomes public so that security guarantees become weaker. But more structures become available, and the mechanisms become more efficient. At lower abstraction levels, the structures become generic, but less information is available to the cloud so that stronger security guarantees could be achieved at the cost of efficiency. Because we aim to design practically efficient mechanisms of secure LP outsourcing, we focus on the top level of the hierarchy. We will study problem transformation techniques that enable customers to secretly transform the original LP into some random one to achieve the secure LP outsourcing design.

Results:



Security:

We now analyze the input/output privacy guarantee under the aforementioned ciphertext only attack

model. Specifically, the only information the cloud server obtains and the obvious fact that A and B of original LP problem are general full rank matrices. Note that in our model no secret transformation key shall be used twice. Offline guessing on problem input/output does not bring cloud server any advantage, since there is no way to justify the validity of the guess. We assume our system uses finite precision floating numbers, and each entry xi of the original solution x should be in range where L with k as our security parameter and poly as a polynomial function.

Conclusion:

Developing a solution over privacy-preserving problem transformation techniques, which allow customers to transform the original LP into some random one while protecting sensitive input/output information. To validate the computation result, we further explore the fundamental duality theorem of LP and derive the necessary and sufficient conditions that correct results must satisfy. Such result verification mechanism is very efficient and incurs close-to-zero additional cost on both cloud server and customers. Extensive security analysis and experiment results show the immediate practicability of our mechanism design.

REFERENCES

[1] C. Wang, K. Ren, and J. Wang, "Secure and practical outsourcing of linear programming in cloud computing," in Proc. IEEE INFOCOM, 2011, pp. 820–828.

[2] P. Mell, and T. Grance, (2011). The NIST definition of cloud computing, Referenced on Nov. 23rd, 2013 [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html#800-145

[3] Cloud Security Alliance. (2009). Security guidance for critical areas of focus in cloud computing [Online]. Available: http:// www.cloudsecurityalliance.org

[4] C. Gentry, "Computing arbitrary functions of encrypted data," Commun. ACM, vol. 53, no. 3, pp. 97–105, 2010.

[5] M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E. H. Spafford, "Secure outsourcing of

scientific computations," Adv. Comput., vol. 54, pp. 216–272, 2001.

[6] S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in Proc. 2nd Int. Conf. Theory Cryptography, 2005, pp. 264–282.

[7] M. J. Atallah and J. Li, "Secure outsourcing of sequence comparisons," Int. J. Inf. Sec., vol. 4, no. 4, pp. 277–287, 2005.

[8] D. Benjamin and M. J. Atallah, "Private and cheating-free outsourcing of algebraic computations," in Proc. Int. Conf. Privacy, Secur., Trust, 2008, pp. 240–245.

[9] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in Proc. 30th Annu. Conf. Adv. Cryptol., Aug. 2010, pp. 465–482.

[10] M. Atallah and K. Frikken, "Securely outsourcing linear algebra computations," in Proc. 5th ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 48–59.

[11] A. C.-C. Yao, "Protocols for secure computations (extended abstract)," in Proc. 23rd Annu. Symp. Found. Comput. Sci., 1982, pp. 160–164.

[12] C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proc. 41st Annu. ACM Symp. Theory Comput., 2009, pp. 169–178.

Author 1:

Mr. Venkatesh Ch he is Pursuing M.Tech CSE in RAMACHANDRA COLLEGE ENGINEERING Eluru, A.P,India

Author 2:

Mr K GOPALA REDDY PROFESSOR HOD Department of CSE, RAMACHANDRA COLLEGE ENGINEERING A.P,India

.