International Journal of Computer Applications (0975 - 8887)
Volume 159 - No.4, February 2017

Secure and Practical Outsourcing of Linear Programming in Cloud Computing: A Survey

V. Sudarsan Rao
Associative Professor
Dept. of CSE
Khammam Inst. of Tech. and Sciences(KITS), (T.S)-India

N. Satyanarayana, PhD
Professor
Dept. of CSE
Nagole Inst. of Tech. and Sciences(NITS), Hyderabad, (T.S)-India

ABSTRACT

How to protect the data that is processed and generated by the customers, is becoming the major concern in the present day situation. Various engineering, computing and optimization techniques are being used to solve this problem. The investigation has been performed for secure outsourcing of problem for the large-scale systems.
In this paper, the essential terms involved in the cloud security has been presented. Whereas, the privacy cheating discouragement "Seccloud", is used for achieving the greater aspects of security. Although the cloud computing is being used to outsource large-scale computations to the cloud, data privacy has become a major issue. In this paper, the modern cryptographic techniques in secure outsourcing along with the research work, which has been proposed in past years, has been presented. Based on some drawback measures, the identification of the problem in the current scenario has been done. This paper also discusses about the motivation towards the problem and our future research directions.

Keywords

Confidential Data, Secure Outsourcing Algorithms, Problem Optimization, Cloud Computing

1. INTRODUCTION

Cloud computing is a computational mechanism, which is used for the convenient non-demand network access to the shared pool of the computing resources which is having the greater efficiency as well as large computational power. Basic advantage of cloud computing is that - it is having the benefits of centralized large computational power, space and efficiency, so that the customers/clients can outsource their complex problem to the cloud for computation purpose. Also, it suffers from the new security challenges like customer's data privacy, confidentiality and checkability. Mostly, the general linear equations of the form $Ax = b$ are the existing computational problem in the scientific community.
Cloud is having the great potential of robust computational power to the aggregated management of the elastic resources. The outsourced problem constraints from the customers' side may contain private and sensitive information eg. personal identifiable business information, sensitive research data etc. So to protect this data from unauthorized use, customers need to encrypt their data prior to outsourcing, but further performing the computations on this encrypted data makes a very hard problem for the cloud server. While on another end, the operations which are being performed may not transparent to customer, so customer needs to verify the result of the outsourced problem after the computation is performed. Most significantly, security is a prime concern that prevents the adoption of computation outsourcing in the cloud.
The client-cloud server architecture can be perceived in the figure 1 below:-

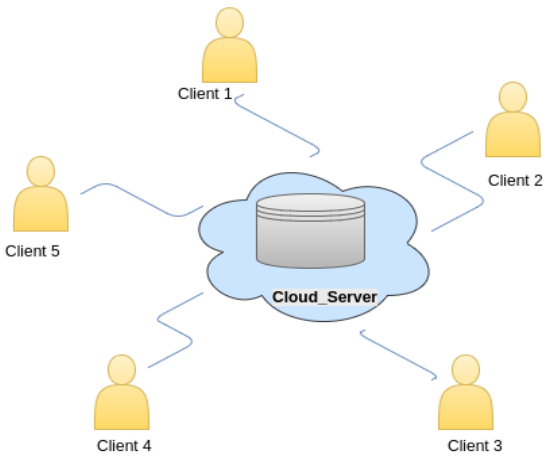

Fig.1

To solve most of the practical optimization problems, Linear Programming(LP) is the most efficient method to adopt. General model of LP problem here, will consists of two LP decompositions - public LP solvers, which will be executing inside the cloud and private LP parameters, which is retained by the customers.

1.1 Motivation to the problem

How to protect customers confidential data(eg. business financial records, personal research data etc.), which has to be prepared and generated during the computation is becoming the major security concern. To resist against unauthorized information leak, sensitive data essentially has to be encrypted before outsourcing. Common data encryption methods in essence limit cloud from performing any meaningful operation of the underlying plaintext data, causing the computation over encrypted data a very difficult problem.

1.2 Organization of the paper

Structure of the remaining paper is as - Section 2 presents some of the preliminaries that are used in this paper. Section 3 explains the overview of some related work. In section 4, the general system computation model has been given. Section 5 of the paper presents the further research directions. Finally conclusions are presented in the section 6.

2. PRELIMINARIES

Some basic preliminaries required in this paper are described as below:-

2.1 Linear Programming

Linear programming is a technique used for maximizing or minimizing a linear function having several variables, with the help of given system constraints. This linear function is called as the objective function, which we seek to maximize or minimize in our feasible region. Feasible region can be defined as a space in which we seek a point that maximizes or minimizes the objective function. So, the optimal solution will always lie inside this feasible region.
The real time optimization problem is usually formulated as the mathematical programming problem and the problem can be expressed in the below form -
minimize, $Z^T y$, subject to $Ay = b$; $y \geq 0$
where,
y: $(n \times 1)$ vector for variables
A: an (m x n) matrix
Z: $(n \times 1)$ column vector
b: $(m \times 1)$ column vector
Some basic techniques for performing Secure Outsourcing of Linear Programming in Cloud are as below:-

—Hiding Equality Constraints
—Hiding Inequality Constraints
—Hiding objective functions

2.2 General Cryptographic Techniques

Cryptography is the science of secret writing. It is a process of storing and transmitting data in an unoriginal form, so that only those person, for whom it was meant, can read and process it. Cipher is a secret method of writing messages, where plaintext is transformed into a cipher text. Converting plain text into cipher text is called encryption and converting cipher text into plain text is called decryption.

2.2.1 Symmetric key cryptography. Symmetric key cryptography relates to the encryption method in which both the sender and receiver use to share the same key. These are realized as either Block ciphers or as Stream ciphers. A block cipher takes blocks of plain text as the form of input, whereas individual characters are taken as input, in case of stream ciphers. Data Encryption Standard(DES) and Advanced Encryption Standard(AES), both are the block cipher designs that have been selected as cryptography standards.
Symmetric key cryptosystems use the same key for both encryption as well as decryption of a message, though a message or collection of messages may have different keys. A notable disadvantage of symmetric ciphers is that, the key management process becomes necessary to use them securely. Key management consists of creation, distribution and refreshing of the secret keys, involved in the communication.

2.2.2 Public key cryptography. It is also called the asymmetric key cryptography. In this method, sender encrypts the message using receiver's public key and further receiver decrypts the message using his own private key. Public key cryptography technique can be used for implementing the various Digital signature schemes. RSA and DSA are two most popular digital signature schemes. Public-key algorithms are mostly based on the very large computational complexity of *"hard problems"*. Eg. the hardness of RSA algorithm is based on integer factorization problem, while hardness of Diffie Hellman and DSA algorithms is based on discrete logarithm problem. Recently, elliptic curve cryptography has been evolved, where security is based on the number theoretic problems involving elliptic curves.

2.3 Modern Cryptographic Techniques in Secure Outsourcing

2.3.1 Homomorphic Encryption. This is a special form of encryption that allows the computations to be performed on ciphertext itself, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext.
There are numerous partially homomorphic cryptosystems as well as fully homomorphic cryptosystems. Fully homomorphic encryption(FHE) is considered to be more secure than partially homomorphic encryption.

—**Partially Homomorphic Encryption:** A cryptosystem is thought as partially homomorphic if it manifests either additive or multiplicative homomorphism property, but not both. Some examples are - RSA(based on multiplicative homomorphism), Paillier(based on additive homomorphism), ElGamal(based on multiplicative homomorphism).

—**Fully Homomorphic Encryption:** A cryptosystem is thought as fully homomorphic if it manifests both additive and multiplicative homomorphism property. The first (and currently only) before-mentioned system is a lattice-based cryptosystem which was in 2010, proposed and developed by Craig Gentry.[15] FHE is considered as far more powerful and a great way to secure the outsourced data in an efficient manner.

—**Ring Homomorphism:** Let, P and Q are rings a function $f : P \rightarrow Q$ will be ring homomorphism if $\forall x_1, x_2 \in P$.
—$f(x_1 + x_2) = f(x_1) + f(x_2)$
—$f(x_1 * x_2) = f(x_1) * f(x_2)$
—$f(1_P) = 1_Q$

3. RELATED WORK

In this section, we will review some existing methods which have been proposed in past years. Atallah et. al. [1][2] has given the general computational methods for securely outsourcing of linear algebraic equations. They have also presented several real time problems for secure outsourcing of complex matrix multiplication and quadrature scientific computations. They have also mentioned the possibility of leakage of confidential and private information. Atallah and Li [3] presented an efficient protocol to securely outsource the sequence comparisons between two servers to overcome the problem of computing using the edit distance between two sequences. Peeter Laud et. al. [4] discussed an arguement of the

impossibility/possibility of outsourcing linear programming. Benjamin and Atallah [5] discussed the difficulty of secure outsourcing for broadly applicable linear algebra calculations. However, the proposed protocol demands the costly operations of homomorphic encryptions.
In past recent years, Wang et. al. [6] introduced a secure outsourcing tool for solving the large-scale system of the linear equations, which is based on the iterative approaches. However, it needs multi-round co-operations between the client and the cloud server and thus is quite impractical. Wang et al. [7] introduced effective mechanisms for secure outsourcing of linear programming computations. But the solution demands various matrix to matrix operations, which will posses cubic-time computational complexity, so is less feasible to apply in practical scenarios. Cong and Ren [8] implemented the mechanism to overcome the problem of securely outsourcing large scale linear equations in the cloud computing by utilizing iterative processes, they also investigated the algebraic characteristic of the matrix multiplication and developed an efficient and effective cheating detection scheme for strong result verification. Lifei and Zhu [9] proposed the SecCloud, protocol which is employed for the data security and privacy in the cloud computation environment as well as it is the combination of data storage security and computation auditing security in the cloud. To enhance the efficiency, several different client's requests can be handled by the batch verification.
Chen and Huang [10] suggested the secure outsource algorithm for the large scale systems. This is suitable for any non-singular non-sparse matrix. Any classic design forms on secure and reliable outsourcing of scientific computations, sequence comparisons and matrix multiplication hardly possible to apply practically in an efficient way, especially for large problems. In those methods, either heavy cloud-side cryptographic computations are involved [12][13] or huge communication complexities [14][17] are required.

4. SYSTEM MODEL

The general architecture and system model of secure outsourcing linear programming problems in the cloud computing is shown as figure 2 below:-

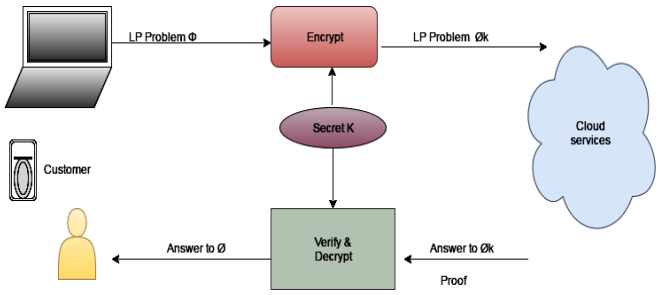

Fig.2

In this model, customers are having the practical optimization problem to solve. But since customers are not having the enough resources to solve that task. Hence customer will direct/outsource the problem in encrypted form, using secret key k, to the server.
General model of LP problem here, will consists of two LP decompositions - public LP solvers, which will be executing inside the cloud and private LP parameters, which is retained by the customers. Then server will use it's public LP solver to solve that task and also produces the proof of the problem. Further server send that solution along with the proof to the customer. On the other end, customer will use it's secret key k for mapping output into the sought answer of his original problem.
Four algorithmic processes (RandomKeyGeneration(RKG), ProblemEncryption(PE), ProofGeneration(PG), ResultDecryption(RD)), which are running inside the system are briefly explained below:-

—RKG$(1^k) \rightarrow \{K\}$ - (This process runs on client side)
  —It is randomized key generation step.
  —It is taking a system security parameter k, and returns a secret key K.
  —K obtained later used by customer to encrypt the target LP problem.

—PE$(K, \phi) \rightarrow \{\phi_K\}$ - (This process runs on client side)
  —Using secret key K, it encrypts ϕ into ϕ_K.
  —ϕ_K will be having same form as ϕ(According to problem transformation).

—PG$(\phi_K) \rightarrow \{y, \Gamma\}$ - (This process runs on cloud server side)
  —Problem ϕ_K is solved and produces both, output y and proof Γ.
  —The output y will be later decrypted to x.
  —Later Γ is used by client for verifying the correctness.

—RD$(K, \phi, y, \Gamma) \rightarrow \{x, \perp\}$ - (This process runs on client side)
  —This algorithm step may choose to verify either y or x with the proof Γ.
  —A correct output x is produced by decrypting y using K.
  —Algorithm outputs $\perp$ when the validation fails.(means server is not doing computation faithfully)

5. RESEARCH DIRECTIONS

Linear programming(LP) is a kind of computational mechanism which takes the first order effects of various system parameters that has to be optimized, and is necessary to the engineering optimization. Based on the advancement in this area, which has been done in past years, we have identified the main problems and drawbacks in the present system. The problem identification and further future research directions are presented as follows:-

5.1 Problem Identification

Today, data privacy and security becomes an essential part of various cloud based applications, multiparty computation scenarios etc. Due to lack of computational resources, clients need to direct their computational problem parameters to cloud. But, security, privacy and confidentiality of client's private data in this whole outsourcing process is a big challenge. The core problems, which we have identified in the present existing system are as below -

—To resist against unauthorized information leakage, sensitive data has to be encrypted before outsourcing. Ordinary data encryption techniques, in essence, prevent the cloud from performing any meaningful operation of the underlying plaintext data, making the computation over encrypted data, a very harsh problem.

—Also, customers are not aware of the computation which is running inside the cloud. So, from customer side, it is also some problem to verify and ensure the correctness of computational results.

5.2 Future Research Directions

Security and privacy of data, specially in clouds, has become most essential part for various applications in present scenario.
Research directions are presented as points below -

(1) To come up with a new Fully Homomorphic encryption(FHE) scheme and apply it to secure computation outsourcing in cloud. Fully Homomorphic Encryption is an special form of encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext.
—Fully Homomorphic encryption(FHE) is a tremendous way to perform processing and computations on the encrypted data in cloud environment, which is being used by any third parties without the knowledge of private secret key.

—Lets the FHE scheme, where -
the encryptions on the plain text M_1 and M_2 can be $Encr(M_1)$ and $Encr(M_2)$. Now, since FHE acheives both additive and multiplicative properties, so both $Encr(M_1 + M_2)$ and $Encr(M_1 * M_2)$ can be computed in a secure and efficient manner. Thus Fully Homomorphic encryption fulfills the purpose of secure outsourcing of customer's problematic data in a great extent.

(2) Since, customers are not aware of the computation which is running inside the cloud. So, from customer side, it is also some problem to verify and ensure the correctness of computational results. So, we will come up with a scheme, which will be having the proof of correctness for the particular outsourced computational problem in the cloud environment.

6. CONCLUSION

Linear Programming has been widely used in various engineering disciplines that analyze and optimize real-world systems, eg. data packet routing, flow control, power management of data centers, etc. There also exist a much powerful thrust to provide the security at various infrastructure levels, while any outsourced computing or any third party computations are being performed. Customers need to outsource their problem to the cloud server for computation in a secure manner, that brings new challenges for customer's data privacy and confidentiality. This paper presents the general system model, an overview of linear programming problem, state of the art in this area and the general architecture of secure outsourcing linear programming problems in cloud computing. The problem identification in this area has also discussed in this paper and have given the future research directions.

7. REFERENCES

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

[2] M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E. H. Spafford, Secure outsourcing of scientific computations, Adv. Comput., vol. 54, pp. 215?272, Jan. 2002.

[3] M. J. Atallah and J. Li, Secure outsourcing of sequence comparisons, Int. J. Inf. Secur., vol. 4, no. 4, pp. 277?287, Oct. 2005.

[4] Peeter Laud, Alisa Pankova, On the (Im)possibility of Privately Outsourcing Linear Programming, ACM, (CCSW'13), November 8, 2013.

[5] D. Benjamin and M. J. Atallah, Private and cheating-free outsourcing of algebraic computations, in Proc. 6th Annu. Conf. Privacy, Secur. Trust (PST), Oct. 2008, pp. 240?245.

[6] C. Wang, K. Ren, J. Wang and Q. Wang, Harnessing the cloud for securely outsourcing large-scale systems of linear equations, IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1172?1181, Jun. 2013.

[7] C. Wang, K. Ren and J. Wang, Secure and practical outsourcing of linear programming in cloud computing, in Proc. 30th IEEE Int. Conf. Comput. Commun. (INFOCOM), Apr. 2011, pp. 820?828.

[8] Cong wang, kui Ren, Harnessing the cloud for securely solving large scale systems of linear equations, Distributed computing systems (ICDCS), 2011 31st International conference on 20-24 june 2011.

[9] Lifei wei, Haojin Zhu, security and privacy for storage and computation in cloud computing, information sciences 258 (2014) 371-386.

[10] Xiaofeng Chen, Xinyi Huang, New Algorithms for Secure Outsourcing of Large-Scale Systems of Linear Equations, IEEE transactions on information forensics and security, vol. 10, no. 1, january 2015.

[11] Cong Wang, Secure Optimization Computation Outsourcing in Cloud Computing: A Case Study of Linear Programming, IEEE transactions on computers, vol. 65, no. 1, january 2016.

[12] P. Mell and T. Grance, Draft nist working definition of cloud computing, Referenced on Jan. 23rd, 2010 Online at http://csrc.nist.gov/groups/SNS/cloud-computing/index.html, 2010.

[13] S. Hohenberger and A. Lysyanskaya, How to securely outsource cryptographic computations, in Proc. of TCC, 2005, pp. 264?282.

[14] R. Gennaro, C. Gentry and B. Parno, Non-interactive verifiable computing: Outsourcing computation to untrusted workers, in Proc. of CRYPTO, Aug. 2010.

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

[16] P. Golle and I. Mironov, Uncheatable distributed computations, in Proc. of CT-RSA, 2001, pp. 425?440.

[17] S. Yu, C. Wang, K. Ren and W. Lou, Achieving secure, scalable, and fine-grained access control in cloud computing, in Proc. of IEEE INFOCOM?10, San Diego, CA, USA, March 2010.