Asian Journal of Convergence in Technology Volume V Issue I
ISSN NO: 2350-1146 I.F-5.11

Secure Outsourcing of Linear Programming Solver in Cloud Computing: A Survey

Prof. S .A. Bhagwat , Assistant Professor in Computer Department

Dr. G. M. Bhandari HOD, Professor in Computer Department

JSPM’S Bhivrabai Sawant Institute of Technology & Research,Pune

Abstract - **There are currently major concerns about how to safeguard and process the data processed by infection. Innumerable industrial, figuring and optimization methods are being used to resolve this problem. The problem has been fixed for secure outsourcing for large issues. In this paper, the terms required in Cloud Security have been presented. The privacy feats of secure cloud are used to frustrate, to achieve more aspects of security. While cloud computing is being used to outsource large scale computer outsourced to the cloud, data privacy has become a major problem. In this paper, modern cryptographic techniques, which have been sourcing with research work proposed in the previous years. Based on some flaw fixes, the current situation has been identified. There is also the motivation for this paper problem and future research guidelines.**

Keywords - Confidential Data; Secure Outsourcing Algorithms; Problem Optimization; Cloud Computing

I. INTRODUCTION

Cloud computing is a computing system that is used for access to convenient non demand network in shared pools of computer resources, which has greater efficiency and greater computing power. The basic advantage of cloud computing is the advantages of centralized large computational power, space and efficiency, so that customers can outsource the cloud to compile your complex problem. Also, this is also due to new security challenges like tight-tuner data privacy, privacy, and inspection. Often, the general linear equations of the X = B form are problems related to the current scientific community.The cloud has the flexibility of flexible management with the flexibility of flexible computing power. Problems extinguished by customer problems, limited private and sensitive information such as Personal identifiable bus information, sensitive search data, etc. Therefore, to protect this data from unauthorized use, customers must encrypt their data before outsourcing,But calculation of computations on these encrypted data makes it a difficult problem for the cloud. On the other side, operations that are operating on the other side may not be transparent to customers, so the customer needs to verify the results of the outsourced issue after computing. Most importantly, security is a major concern, which prohibits the adoption of outsourcing in the cloud. In order to solve a practical optimization problem, Linear Programming (LP) is the most effective way of accepting it. There will be two LP decompositions in the general model of the LP issue - public LP solver, which are working in the cloud and private LP parameters, which are maintained by the customer.The client-cloud server architecture can be perceived in the figure below:-

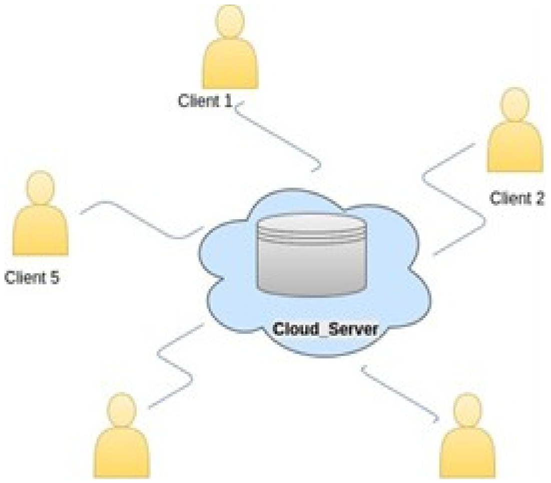

Fig:1 Client server Architecture

A. Motivation to the problem

Customers must be prepared and generated during the calculation to protect confidential data (e.g., business financial records, personal research data, etc.). Against unauthorized information leaks, sensitive data must be encrypted before essential outsourcing. Due to the general limitations of standard data encryption methods in the cloud, it is a difficult problem to calculate encrypted data.

B. Organization of the paper

Structure of the rest of the paper is as - Section 2 gives some of the introductions that are used in this paper. Section 3 explains the outline 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.

II. PRELIMINARIES

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

A. Linear Programming

Linear programming is a technique that is used with the help of system restrictions, to increase linear function with multiple steps or to small scale. This linear function is known as an objective function, which you try to maximize or decrease in your potential area. The viable area can be defined as a place in which you can find such points in which the maximum number of objectives will be reduced or decreased. So, there will always be satisfactory solution in this viable area.Real time optimization problems are usually created as a mathematical programming problem and the problem can be describe in the form below

minimize, $Z^T y$, subject to $Ay = \geq b$; y 0 (1)

where,

y: ($\times n$ 1) vector for variables

A: an (m x n) matrix

Z: ($\times n$ 1) column vector

b: ($\times m$ 1) column vector

Some basic techniques for performing Confident Outsourcing of Linear Programming in Cloud are as below:-

1. Hiding Equality Constraints
2. Hiding Inequality Constraints
3. Hiding objective functions

Let us define some terms used in Linear Programming .

- Decision Variables: The decision variables are the variables which will decide the output. They represent my ultimate solution. To solve any problem, we first need to find the decision variables.
- Objective Function: It is defined as the objective of making decisions.
- Constraints: The constraints are the restrictions or limitations on the decision variables. They usually limit the value of the decision variables.
- Non-negativity restriction: For all linear programs, the decision variables should always take non-negative values.

B. General Cryptographic Techniques

Cryptography is the science of secret writing. This is a process for storing and transmitting data in an informal form so that it can read and process only the person that they meant. Cipher is a secret way of writing a message, where plain text is converted to a cipher text. Converting a plain text into a cipher text means encryption and conversion cipher, which is called decryption as text .

1. Symmetric key cryptography.

Symmetric cryptography is related to encryption methods in which both senders and recipients are used to share the same key. These are considered as block ciphers or stream ciphers. Block cipher is taken as plain text block in the form of input form, whereas in case of flow cipher individual characters are taken as input. Data Encryption Standard (DES) and Advance Encryption Standard (AES), are block cipher designs that have been selected as cryptography standards. Symmetric cryptosystems use the same key for both encryption and decryption of messages, however the message's message or archive may have different keys. One notable loss of symmetric cipher is that it requires key management processes to be used. Includes secret key generation, distribution, and refreshments included in the main management communications.

2. Public key cryptography.

It is also called asymmetric cryptography. In this method, the sender enters the recipient's public key message and decrypts the next recipient message using its own private key. Public digital cryptography techniques can be used to implement various digital signature schemes. RSA and DSA are the two most popular digital signature schemes. Public key algorithms are based on a large complexity of most "difficult problems". For example, while the RSA algorithm's strictness is based on the problem of the problem, the hardness of Diffie Hellman and the DSA algorithm is based on the problem of the individual logarithm. Recently, the vertical curved cryptography has been developed, where safety is based on theoretical problems involving oval parameters.

3. Modern Cryptographic Techniques in Secure Outsourcing

i. Homomorphic Encryption.

This is a special type of encryption that allows encryption on your computer to be done on a cipher text itself, thus generating encrypted results, which can be matched by the decryption of the result of the operation on plain text. There are innumerable homomorphic cryptosystems as well as a complete homomorphic cryptosystem. Completely Homomorphic Encryption (FHE) is considered to be more secure than partially homomorphic encryption.

- Partially Homomorphic Encryption: A cryptosystem is considered partly as homomorphic if it shows either affinity or multiplied prosperity property, but not both. Some examples - RSA (based on multiplier homomorphism), pyelier (based on the behavioral homomorphism), LGG (based on multiplier homomorphism).
- Fully Homomorphic Encryption: Cryptosystems are considered completely homomorphic if they reveal both couples and multicomotor homomorphic properties. The first (and presently only) system previously mentioned is a mesh-based cryptosystem that was proposed and developed by Craig Gentry in 2010. [15] FHE is considered to be a more powerful and best way to efficiently secure outsourced data.

III. RELATED WORK

In this section, we review some of the current methods proposed in the past few years. Kong and Jia have given a secure outsourcing method to solve the large number of linear equations (LE) systems in the cloud. Use of such traditional practices as a Gaussian emissions or a lu decomposition (aka direct method) will be fatal for a large number of LESs, because we completely create a fully loaded outsourcing system through a different approach-repetition method, in which implementation is very easy to implement. Practice and demand only relatively simple Metrics-vector operations. In particular, As a result of our system, the ALALA will keep the customer's personal input and output private. Etc. To be able to use the cloud to get constant forecasts in LA solution frequently. Al. [1] [2] has given general computing methods for secure outsourcing of linear algebraic equations. They also introduced complex real-time problems for the complex outsourcing of multi-matrix and quadratic scientific computations.

They have also mentioned the possibility of leakage of confidential and private information. Atlah and Lee [3] presented an effective protocol for out-of-the-way safely out-of-the-way comparison of two servers in order to overcome the problem of computer using the editing distance between two sequences. Peter Loud et al. Al. [4] One debate was discussed. The possibility of exposure / outsourcing linear programming Ben-Zamin and Atalah [5] discuss outsourcing safety issues for widely applied linear algebraic calculations. However, the proposed protocol has demanded expensive operations of homomorphic encryption.

In the past few years, Wang et. Al. [6] Launched a secure outsourcing device to solve a large number of linear equations, which is based on revised approaches. However, multi-co-operative collaboration between client and cloud server is required and that is why it is impractical. Wang et al. [7] Effective match-animation was introduced for safe outsourcing of linear programming computers. But satisfactorily, the demand for different matrices in the Matrix operance, in which there is a cubic-time computing complexity, can not be applied in practical situations. Kong and Rain [8] have implemented this technology by using a repeating process to overcome the problem of securely outsourcing large numbers of linear equations in cloud computing. He inspected the algebraic properties of matrix properties and developed effective and effective fraud detection plans. Strong results for verimpication. Life and Zhu [9] have proposed the Secure Cloud Protocol that is used for data security and privacy in cloud computing environments, as well as a combination of data storage security and auditing security in the cloud. To increase performance, many different client requests can be handled with batch verification.

Chen and Huang [10] indicate a secure outsourcing algorithm for large scale systems. This is suitable for any non-abnormal sparse matrix. For any classic design form on safe and reliable outsourcing of scientific computations, especially for larger issues, effectively comparing sequence and matrix multiplication possible is possible as possible. In such cases, there is either cloud-side cryptographic computation, [12] [13] or massive communication complexity [14] [17].

IV. SYSTEM MODEL

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

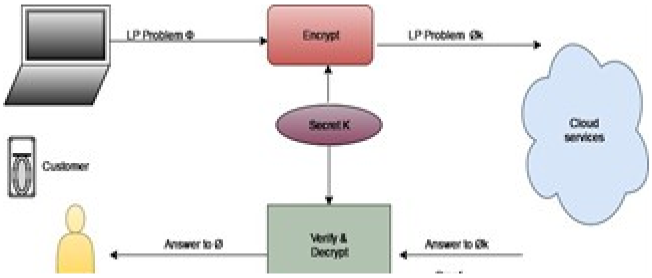

Fig.2 System model of secure outsourcing of linear programming

In this model, customers are having practical optimization problems to solve. But customers do not have enough resources to solve that action. That's why customers will outsource the problem to the server / encrypted form directly, using the Confidential Key key. There will be two LP decompositions in the general model of the LP issue. Public LP Solars, which will be working in Claude and Private LP Parameters, are maintained by the customers. Then the server will use that public solution and also make it easy to work. The next server will send the solution to the customers with proof. On the other hand, the customer will use the secret key for mapping output in response to the demand for its original problem.

Four algorithmic processes (Random Key Generation(RKG), Problem Encryption(PE), Proof Generation(PG), Result Decryption(RD)), which are running inside the system are briefly explained below:-

- RKG(1^k) K - (This process runs on client side)
- It is randomized key generation step.
- It is taking a system safety factor k, and returns a secret key K.
- K attained later used by client to encode the target LP problem.
- PE(K, φ) φ_K - (This process runs on client side)
- Using secret key K, it encodes φ into φ_K.
- φ_K will be taking same procedure as φ(According to problem transformation).
- PG(φ_K) y, Γ - (This process runs on cloud server side)
- Problem φ_K is explained and produces both, output y and proof Γ.
- The output y will be later decrypted to x.
- Later Γ is used by client for confirming the

perfection.

- RD(K, φ, y, Γ) x, - (This process runs on client side)
- This procedure step may choose to prove either y or x with the proof Γ.
- A right output x is produced by decrypting y using K.
- Algorithm outputs when the proof fails. (means server is not doing computation faithfully)

V.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 additional future study guidelines are presented as follows:-

A. *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, customers 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 -

1. To resist against illegal 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 encoded data, a very harsh problem.
2. Also, clients 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.

B. *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. For the first time, we utilize the sparse matrix to propose a new protected outsourcing procedure of large-scale linear equations in the fully malicious model.
2. Since, clients 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 system, which will be having the proof of accuracy for the specific outsourced computational problem in the cloud environment.

VI. CONCLUSION

Linear programming has been used extensively in many engineering departments that analyze and optimize real-world systems, e.g. Data packet routing, flow control, power management of data center, etc. There is a very strong emphasis on providing security at various structural levels during various outsourcing computing or any third party computations. Clients need to outsource their problem to securely measure customers, This results in new challenges for consumers' data privacy. This documentation presents a common system model, observation of linear programming problem, the state of the art in this field and the common architecture of secure outsourcing linear programming issues in cloud computing. In this area, discussion has been discussed in this paper to identify problems and future research guidelines are given.

VII. REFERENCES

[1] M. Atallah and K. Frikken, Securely outsourcing linear al- gebra 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 com- parisons, Int. J. Inf. Secur., vol. 4, no. 4, pp. 277?287, Oct. 2005.

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

[5] D. Benjamin and M. J. Atallah, Private and cheating-free out- sourcing 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 equa- tions, 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 outsourc- ing 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 solv- ing large scale systems of linear equations, Distributed com- puting 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 out- source cryptographic computations, in Proc. of TCC, 2005, pp. 264?282.

[14] R. Gennaro, C. Gentry and B. Parno, Non-interactive verifi- able computing: Outsourcing computation to untrusted work- ers, 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 computa- tions, in Proc. of CT-RSA, 2001, pp. 425?440.

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

[18] Cong Wang,Jia Wang, Harnessing the Cloud for Securely Outsourcing Large-Scale Systems of Linear Equations in IEEE trans.on parallel and distributed systems,Vol 24,no. 6