

Secure Outsourcing of Linear Optimization in Cloud Computing

Banoth Ravi¹, R.Vijayaprakash²

¹Department of CSE, SR Engineering College, Warangal, Andhra Pradesh, India

²Associate Professor, Department of CSE, SR Engineering College, Warangal, Andhra Pradesh, India

Abstract: Cloud computing has become a reality which is capable of enabling general public and organizations to make use of huge computational resources without capital investment in pay per use fashion. This new paradigm allows customers who have no much computational resources to outsource their expensive computational workloads to cloud and get the benefits of its storage, servers, networking and other facilities. Thus cloud computing has unlimited possibilities as one can feel world class infrastructure and facilities in her own computer sans investment. Though the provision to outsource computationally expensive workloads to cloud, there is concern about security that make people think before using cloud for this purpose. This is because basically Internet and associated infrastructure is conceived as untrusted. Though cloud service providers take care of security customer have their own concerns with respect to protection of their sensitive data. Therefore, it is required to have secure mechanism to protect data of customers and also ensure that the results are properly validated. This will enable customers to outsource their works fearlessly. The complete communication should take place in encrypted format. This is practically a challenging problem. This paper focuses on the Linear programming computations that take place over cloud with complete security. The proposed system takes care of data security while it is in transit and also has mechanisms to support verification of data for correctness. The empirical results reveal that the proposed system is practical and can be used in the real world systems. It is also found that the result verification of the system is computationally efficient does not incur additional cost.

I. INTRODUCTION

Cloud computing is an emerging technology that enables people to access state – of – the – art computational resources in pay per use approach without the need for capital investment. The cloud computing is made available in many ways. They are Infrastructure as a service (IaaS), Platform as a service (PaaS), and Software as a service (SaaS) [1]. Cloud customers' systems are resource constraint. However, with cloud computing and virtualization technologies, they do not feel so as they are virtually connected to unlimited configurable computing resources of the cloud. Customers of cloud have access to such resources in pay per use manner that leads to cheaper availability of resources. This paves the way for businesses to have possibilities for greater achievements in profits as they are provided with huge resources seamlessly integrated through Internet. This phenomenon which was envisaged in 1960's has been made a reality now and it is able to cater the needs of customers without letting them purchase hardware, software and also eliminates operational or maintenance overhead. By outsourcing the computationally expensive workloads, the customers can have many advantages that are usually with cloud computing.

In spite of these benefits, customers outsourcing their valuable computations (along with data) to cloud with respect to Linear Programming are worried about the security of their data. Moreover the customers have no direct control over these operations [2]. The results of such outsourcing also contain sensitive information that has to be protected. The result needs to be verified for its correctness too. Sensitive data has to be encrypted before outsourcing so as to ensure confidentiality. At the same time the encryption techniques also prevent cloud from making computations [3]. The computations done in the cloud server solve LP computational problems. However, such operations are not transparent to cloud customers. This may help cloud service provides to indulge in unethical practices. This may lead to incorrect results, semi-honest models, inappropriate storage facilities and so on [4]. In addition to this cloud server may have software and hardware bugs that add to the severity of the problem as it can lead to attacks from hackers and intruders. For this reason the cloud is insecure from the viewpoint of its customers though in may be very secure from the view point of service providers. Based on its economic nature, cloud customers have to risk security as the inputs and outputs are to be securely transmitted and also the integration of the result is so important. For this reason any practical solution of cloud should consider all these issues in the design. If the data of customers is not safeguarded, they do not make use of cloud for outsourcing LP problems [5-10]. From the literature it is understood that [11], and [12] are having solutions for this problem. They are based on circuits and homomorphic encryption schemes respectively. As per general theory provided in literature, it is viable to outsource linear programming to cloud. However, this

can't be relied up on unless a most secure mechanisms which provides end to end security solutions in the process of outsourcing. The circuits solution is used with encrypted private inputs but this is far from practical in the real world and FHE is proved to be highly complex with pessimistic circuit sizes which are not practically feasible. This is the motivation for this paper to find out a feasible solution that overcomes these setbacks. Many solutions including the above two available in the literature are computationally expensive with heavy cloud – side cryptographic computations or huge communication complexities involved.

In this paper efficient mechanisms for linear programming by focusing on optimization techniques and engineering computing. Linear programming tasks need large amount of RAM and processing power. As they are not available in client system, the cloud clients out source them. In various engineering streams, this is required and it has been done. The tasks that analyze and optimize have to use LP in engineering computing [13]. In the proposed system the customer's LP problem is formulated as a collection of matrices and vectors. A set or privacy preserving techniques is possible to be applied on them as they are high level representations. The high level representations include affine mapping and matrix multiplication. These representations help to transform original LP problem into some intermediate and sensitive I/O. The advantage of using these representations is that the cloud servers can reuse existing solutions that work on these representations. The transformed LP problem is solved by cloud server and assuming that the validations of computation result is performed. We make use of both LP problem and the basic duality theorem together in order to arrive at required criteria that the results must satisfy. This kind of approach results in zero computational cost additionally on both cloud server and cloud customer. When the result is correct and verified, the customer can utilize the secret information map to the required solution for the original LP problem given by the customer. The proposed architecture is as given in figure 1.

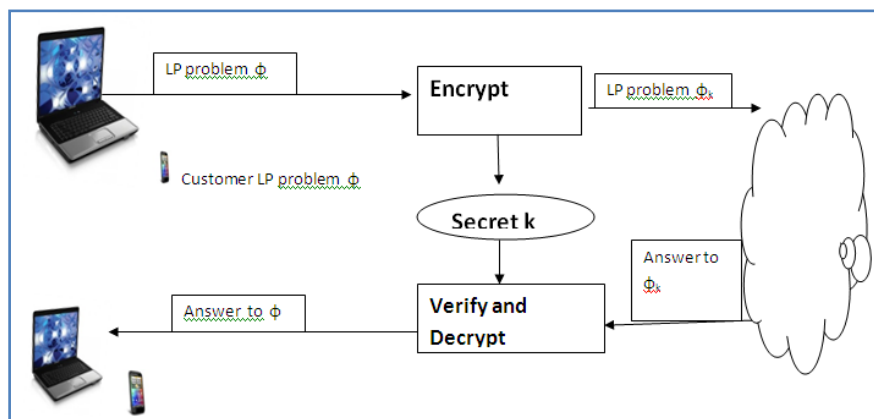


Fig. 1: Architecture for Secure Outsourcing of LP

As seen in fig.1, customer gives LP problem. The proposed system encrypts it and the encrypted LP problem is sent to cloud server. In the cloud server, the outsourced LP problem gets computed and the result is given back to user along with verification details. Thus the user can establish the integrity of the information he receives.

II. RELATED WORK

There has been research on outsourcing of computation and its security. The feasibility of this is established in [9] theoretically. The feasibility includes the generation operations including input, output, and guarantee of correctness and so on. In spite of the soundness of the theory proposed in [9] to demonstrate feasibility of secure computation outsourcing, it is unduly complex and can't be used practically. At least the fact is that it is not currently being used by industry. By customizing the construction of circuits, Atallah et al. explored on secure outsourcing of specific applications as discussed in [5], and [8]. The first research has been reviewed in [5] on secure computation outsourcing of scientific and numeral computations. The scientific applications like string pattern matching, sorting, linear algebra etc. are explored and solved by using a set of techniques based on the problem domain. Information disclosure is the problem faced in these solutions. In addition to that they also cannot handle verification of result. Our work is able to that and also the result verification is managed to have almost zero additional cost on the system. For two different types of tasks such as secure algebraic computation outsourcing and secure sequence comparison outsourcing Atallah et al. developed two protocols respectively. Both the protocols heavily depend on cryptography and also oblivious transfer as explored in [14] and [15]. The problem with these protocols is that they can't scale well with large problems. The experiments on these protocols calls on done on systems without considering collusion attacks. Therefore they may be vulnerable to such attacks.

Of late in [10] secure computation outsourcing is proved which is based on matrix multiplications and secret sharing [16]. This work does not use cryptographic primitives and computationally efficient. In spite of this some sort of computational overhead is there as the scalar operations are expanded to polynomials. In this case the cost of results verification is more even as some pre-computing noise matrices are to be introduced. The solutions mentioned so far are elegant. However, they are not practical and immediately they can't be used in the real world. This drawback is overcome in this paper. Other work that is somewhat similar to our work is in [11] which are on Secure Multi-party Computation (SMC) which can be used by two or more parties to solve problems and at the same time not disclosing one user's information to another user. In [17] customized solutions of SMC such as sequence comparisons, scientific computations etc. These techniques are used in general without computing. Applying them to cloud computing environment is problematic. This is because they are developed without keeping the asymmetry among the cloud servers and cloud customers and also security problems. The complete input information is not known to the parties in SMC and thus verifying result is made difficult here. When compared to this our approach enables customers to have complete input information and the facility of result verification too.

In [18] Atallah and Li did first research on linear programming with collaborative and secure communication. The limitation of this work is that it can't work for large size real world problems and could not get an optimal solution. The same framework has been enhanced by Toft [19] where he proposed Simplex algorithm which has been revised in [20] based on two protocols namely secure comparison and secure scalar product. Almost all solutions work for small sized projects relatively. Another issue with respect to them in general is computation asymmetry and hence they are not directly suitable for computation outsourcing securely. Especially they can't be directly used with cloud computing. Our solution scales for large problems and works in cloud computing environments with result verification support that incurs zero additional computational overhead.

III. PROBLEM STATEMENT

The system and the threat model are visualized in fig. 1. As seen in fig. 1, it is evident that there are two parties involved. They are known as cloud customer and cloud server. The cloud client is supposed to send LP problems to cloud server. The cloud server is expected to have LP solvers that can be used by public for various LP problems encountered by them. The cloud server also deals with cryptographic primitives and the security is provided. The cloud server also takes care of returning solution to LP problem and also verification mechanism for helping the cloud customer to establish integrity of his inputs and outputs effectively. Here the system model is that cloud customer get LP problem solving services in pay per use fashion without investing on the infrastructure. Secure outsourcing is thus made possible and the rest of the paper will elaborate on these lines more. Here the cloud customer is considered genuine. It is assumed that cloud server might have malicious behavior. This is like a semi – honest model in terms of CS. This assumption is made by earlier researches such as [21] and [22]. As part of this model, the CS might be interested in analyzing sensitive information that is flown between customer and CS. Another assumption is that the communication channels between them are realizable authenticated in order to gain performance pertaining to security. For this reason aspect such as secure authentication is omitted in the presentation of this paper entirely.

The design goals of the proposed system are CS should provide results that can be verified for integrity of information; CS is not supposed to generate any kind of incorrect output; cloud customer's private data has to be protected by CS. This does mean that cloud server should not obtain any sensitive information of the customer when the process is going on; efficiency in terms of time and cost should be more when cloud server computes LP problems.

Linear Programming

It is nothing but a mathematical programming problem that expect various decision variables to participate in the computations and minimize objective function which is offline function with respect to decision variables. A linear problem can be expressed as follows.

$$\text{minimize } c^T x \quad \text{subject to } Ax = b, Bx \geq 0.$$

IV. PROPOSED SOLUTION

The proposed mechanism design framework for outsourcing LP problem to cloud server and getting results with security constraints in place with verification mechanism. This is the general framework described in [9]. However, our way of instantiation of security constructs is different. We propose four algorithms to achieve mechanism described in figure1. The cloud server should use an algorithm by name ProofGen while the other algorithms such as KeyGen, ProbEnc, and ResultDec.

The KeyGen which runs at client is a randomized algorithm for secure key generation. It takes a security parameter from system (k) and returns a key known as secret key. This key thus generated is used by customer later in order to encrypt his LP problem before sending it to cloud server. ProbEnc algorithm is responsible to encrypt input at customer side using secret key generated using KeyGen algorithm. The encrypted content forms the actual problem to be solved by public LP solvers deployed in cloud server. ProofGen is an algorithm that is responsible to generate adequate proof of the integrity of customer's data and solution. This algorithm is executed at CS. ResultDec is an algorithm executed at client in order to verify the data sent by CS. This ensures the effective and secure outsourcing of LP problems to public LP solvers deployed in cloud servers.

Linear Programming

Finding minimum and maximum value of a linear expression is an example for linear programming problem.

$$ax + by + cz + \dots$$

This expression known as objective function is subject to many linear constraints of the form

$$Ax + By + Cz + \dots \leq N$$

or

$$Ax + By + Cz + \dots \geq N.$$

An optimal value is nothing but the smallest of largest value of objective function.

A linear function to be maximized

e.g. $f(x_{\{1\}}, x_{\{2\}}) = c_{\{1\}} x_{\{1\}} + c_{\{2\}} x_{\{2\}}$

Problem constraints of the following form

e.g.

$$\begin{matrix} \backslash \text{begin} \{ \text{matrix} \} \\ a_{\{11\}} x_{\{1\}} + a_{\{12\}} x_{\{2\}} \leq b_{\{1\}} \\ a_{\{21\}} x_{\{1\}} + a_{\{22\}} x_{\{2\}} \leq b_{\{2\}} \\ a_{\{31\}} x_{\{1\}} + a_{\{32\}} x_{\{2\}} \leq b_{\{3\}} \\ \backslash \text{end} \{ \text{matrix} \} \end{matrix}$$

Non-Linear Problem

One of the examples of non-linear problem is of optimizing transportation costs by selecting a group of transportation methods. Out of them one or more will exhibit economics of scale under constraints of various capacities and connectivities. An obvious example is petroleum product transportation to a barge coastal tank ship. In addition to smooth changes, the cost functions may have discontinuities. The general NLO Non-linear optimization problem is to maximize some variable like product throughput or minimize cost function. A two dimensional example is as given below.

The intersection of the line with the constrained space represents the solution

A simple problem can be defined by the constraints

$$x_1 \geq 0$$

$$x_2 \geq 0$$

$$x_1^2 + x_2^2 \geq 1$$

$$x_1^2 + x_2^2 \leq 2$$

with an objective function to be maximized

$$f(x) = x_1 + x_2$$

where $x = (x_1, x_2)$. Solve 2-D Problem

A three dimensional example is given below.

The intersection of the top surface with the constrained space in the center represents the solution

Another simple problem can be defined by the constraints

$$x_1^2 - x_2^2 + x_3^2 \leq 2$$

$$x_1^2 + x_2^2 + x_3^2 \leq 10$$

with an objective function to be maximized

$$f(x) = x_1 x_2 + x_2 x_3$$

where $x = (x_1, x_2, x_3)$. Solve 3-D Problem.

Web Based Prototype Application

A web based prototype application is developed to demonstrate the practical outsourcing of linear and non-linear programming. The application is built using JDK 1.6, Servlets and JSP technologies. The environment used is a PC with 2 GB RAM and 2.9x GHz processor. The main screen of the application is as shown in fig. 2.

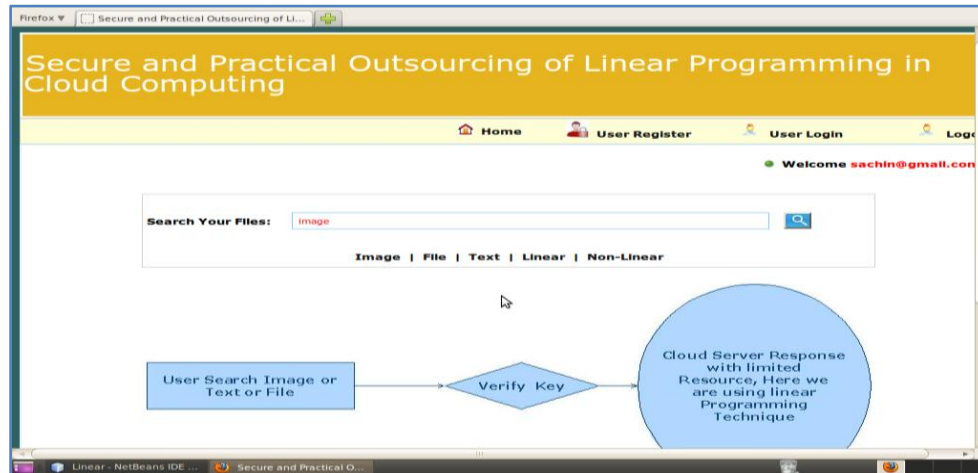


Fig. 2: Main UI of the Proposed System

V. SECURITY ANALYSIS

Our theorems prove that the soundness and correctness of our proposed approach for secure outsourcing of LP problem to cloud. Theorem 1 says that our scheme is verifiable and correct for the purpose of linear programming. The proof given by CS has two parts namely solution is given in encrypted form that has to be decrypted by customer; and the result verification mechanism guarantees that the verification process can establish the correctness and integrity of solution with respect to problem in hand. Theorem 2 says that our scheme is verifiable and sound for secure outsourcing of linear programming in cloud. The verification through offline mapping of input and output proves the soundness of our scheme with respect to security. Therefore the conclusion with respect to security analysis is that, our scheme is secure beyond any doubt.

Privacy of Input and Output

The privacy of input and output should be guaranteed to consider the proposed system for secure outsourcing of LP problems to cloud servers. For this a cipher text attack only model has been devised. The four algorithms described in the previous sub section ensure that privacy and protection of data and result are possible. The breach of security can be identified as there is provision for verification of integrity of solved LP problem.

VI. PERFORMANCE ANALYSIS

Customer side algorithms such as KeyGen, ProbEnc and ResultDec cause computational overhead to some extent. We used efficient models in these algorithms. However, the efficiency can be further increased by using Coppersmith – Winograd algorithm [23]. The proposed scheme has been tested with experiments. The experiments revealed that the system is working as expected and capable of providing secure outsourcing of LP problems. The important difference between previous works and our work in this regard is that the existing works do not provide verification module. Our system provides a verification mechanism that allows cloud customers to check integrity of result in connection with input problem. This helps to increase the usage of cloud for the purpose of secure and practical outsourcing of LP problems. Moreover our system is close to zero additional overhead for verification. The solutions given in [7] and [8] use two protocols namely secure sequence comparison outsourcing and secure algebraic computation outsourcing. However, these are not capable of scaling up for large problem sets. The solution given in [6] also proved to be computationally expensive. Very recent work [10] outperforms previous works as it is more secure. However, its computational overhead is too high to relay on for practical usage.



VII. CONCLUSION

This paper provides a practical solution to the problem of secure outsourcing of Linear Programming. The computations of LP are taken place in cloud as the client has not equipped with such resources. The proposed system is efficient and provides complete security to outsourced computations and the data while transit. The mechanism practically divides the work into private data and public LP solvers. The important aspect of this system is that it not only provides secure data transmission but provides ways and means to verify the correctness of data as well. Thus it is made cheating resilient. The verification mechanism is bundled with the security solution without any additional computational overhead.

REFERENCES

- [1] 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.
- [2] Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, online at <http://www.cloudsecurityalliance.org>.
- [3] C. Gentry, "Computing arbitrary functions of encrypted data," *Commun. ACM*, vol. 53, no. 3, pp. 97–105, 2010.
- [4] Sun Microsystems, Inc., "Building customer trust in cloud computing with transparent security," 2009, online at <https://www.sun.com/offers/details/sun-transparency.xml>.
- [5] M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E. H. Spafford, "Secure outsourcing of scientific computations," *Advances in Computers*, vol. 54, pp. 216–272, 2001.
- [6] S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in *Proc. of TCC*, 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. of 6th Conf. on Privacy, Security, and Trust (PST)*, 2008, pp. 240–245.
- [9] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in *Proc. of CRYPTO'10*, Aug. 2010.
- [10] M. Atallah and K. Frikken, "Securely outsourcing linear algebra computations," in *Proc. of ASIACCS*, 2010, pp. 48–59.
- [11] A. C.-C. Yao, "Protocols for secure computations (extended abstract)," in *Proc. of FOCS'82*, 1982, pp. 160–164.
- [12] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc of STOC*, 2009, pp. 169–178.
- [13] D. Luenberger and Y. Ye, *Linear and Nonlinear Programming*, 3rd ed. Springer, 2008.
- [14] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. of EUROCRYPT'99*, 1999, pp. 223–238.
- [15] S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," *Commun. ACM*, vol. 28, no. 6, pp. 637–647, 1985.
- [16] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.
- [17] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game or a completeness theorem for protocols with honest majority," in *Proc. of STOC'87*, 1987, pp. 218–229.
- [18] W. Du and M. J. Atallah, "Secure multi-party computation problems and their applications: a review and open problems," in *Proc. of New Security Paradigms Workshop (NSPW)*, 2001, pp. 13–22.
- [19] J. Li and M. J. Atallah, "Secure and private collaborative linear programming," in *Proc. of CollaborateCom*, Nov. 2006.
- [20] S. Goldwasser, Y. T. Kalai, and G. N. Rothblum, "Delegating computation: interactive proofs for muggles," in *Proc. of STOC*, 2008, pp. 113–122.
- [21] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in *Proc. of ICDCS'10*, 2010.
- [22] 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.
- [23] D. Coppersmith and S. Winograd, "Matrix multiplication via arithmetic progressions," in *Proc. of STOC'87*, 1987, pp. 1–6.

AUTHORS

	Mr. Banoth Ravi, M.Tech from SR Engineering College, Anantha sagar, Warangal Completed B.Tech from Vaagdevi college of Engineering Bollikunta Warangal interested towards secure and practical outsourcing of LP inCloud Computing.
	R. Vijayaprakash(Ph.D)(Pursuing) and he is Associate Professor in SR Engineering College, Warangal, AP, INDIA. He has received MCA Degree Computers, M.Tech P.G. in computer science and engineering. His main research interest includes data mining. Cloud computing.