RESEARCH ARTICLE OPEN ACCESS

Secure Outsourcing of Linear Programming in Cloud Computing Environment: A Review

Shephali Singh[1],Puneet Sharma[2],Dr. Deepak Arora[3]
Department of Computer Science & Engineering, Amity University, Lucknow

ABSTRACT
Cloud computing provides immense computing power with reduced cost. User can outsource their vast computational work to the cloud and use massive computational power, storage, software, network etc. Despite all these benefits there are still few obstacles in cloud computing regarding confidentiality and integrity of data. Outsourcing and computation compromises the security of data being stored on cloud computing. Considering cloud as insecure platform a system must be designed that protects data by encryption and as well as produces correct result without any cheating resilience with the help of result verification. In this paper, we study the secure outsourcing and computation of linear programming by capturing the effects of arguments which are of first order and that provides practical efficiency. To achieve efficiency linear programming conditions are implemented. The LP computation are done explicitly decomposing LP problem that are run on cloud. The parameters of LP are owned by the customer. For validating the obtained output of computation, we use duality theorem of linear programming that derives the required condition that the result must fulfil.

Keywords**:** Cloud Computing, Data Security, Duality theorem, Linear Programming and Outsourcing.

I. INTRODUCTION

On demand network access is provided by cloud computing such as computing resources and storage of data with more efficiency and less management overhead. The cloud computing has advantage of computational outsourcing where the strength of user is not restrained to its resources or devices. The outsourcing of workloads into cloud provides customer huge computing resources without huge investments in hardware or software purchase. With all these advantages comes the concern of security of cloud platform. The main concern is with the security of data stored in cloud. The outsourced data may contain crucial information such as financial records, research data, military information, personal records etc. The leakage or modification of these data may lead to inevitable changes or problems.

To protect the data outsourced on cloud, encryption of sensitive data must be done. Before outsourcing the data should be encrypted so as to maintain confidentiality of data stored in cloud. Other than encryption, the cloud itself is sometimes not very faithful which may lead to incorrect results. Though it is possible that software bugs, hardware failure or even outsider attack may decrease the result quality. From the viewpoint of customer the cloud is insecure. It would be difficult for customer to give their working control of cloud from the local machine without the assurance of security of their data i.e. to save valuable I/P and O/P information and verify the correctness of result. Cryptographic and computer recent researches have lead to advancement in “safe outsourcing costly computations” (e.g. [1]-[5]). The working of secure computation in cloud has been found to be feasible in theory [6] by Yao’s garbled circuits [7] and Gentry’s research work on fully homomorphic encryption (FHE) algorithm [8] that represents the computation on Boolean circuit as the combination of encryption that can be assessed with the help of inputs that are encrypted. But using this method will be not so practical due to high complexity and large Boolean circuits. Other outsourcing computation method include sequence comparison, matrix multiplication etc. It is still hard to apply them practically in large problems. In these heavy cloud side cryptography computation [3], complexity related to communication [8] are involved.

Here we look into effective methods of outsourcing computations of linear programming safely [9]. However ordinary encryption techniques does not allow cloud to perform any operations of the plaintext data, making it difficult to perform computation over encrypted data. Linear programming works on algorithm that finds the first order effect of different parameters of system that must give optimal solution to increase efficiency. Its usage is in routing of packets, flow control of network, data centres power management etc. [10]. Since linear programming problem requires lot computational resources and it involves very sensitive data that is why it is decomposed and outsourced into LP problem solvers that are public and executing on cloud and LP parameters that are of customers and are private. Vectors and matrices are used to transform LP problems of customer. This transformations makes privacy preserving techniques such as matrix multiplication and affine mapping easily applicable. This allows insecure input and output data to be safe and secure. Other than this, the duality theorem along with bit by bit formation of LP problem derives basic conditions that are required to be correct to satisfy the result. This method to validate the result is very effective and has very less appended overhead on the customer cloud as well as server cloud.

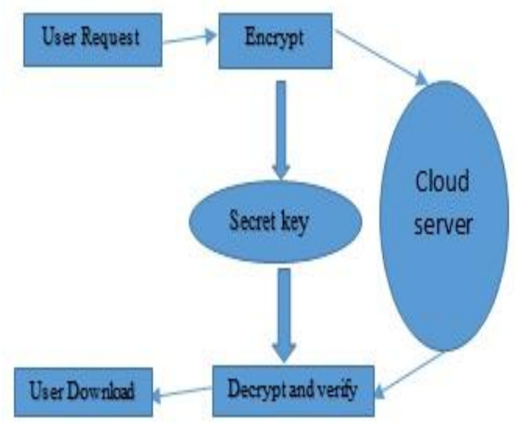


Figure. 1: Pictorial representation of secure outsourcing and computation of LP problem in Cloud.

II.

ITERATURE SURVEY

Researcher Gennaro et al. [5] has shown literary working of secure computation outsourcing. He has shown feasibility of input and output privacy maintenance as well as correctness and soundness of the result. However, it is not practically sound method due to high computing complexity. Later Atallah et al. did a list of works [1] [3] [4] [8] for secure outsourcing computation. The set of techniques used were string matching, linear algebra, sorting etc. However, these mechanism were not very efficient in securing input and output information and did not confirmed correctness of result, which is the main concern in secure computation on cloud. Atallah et al. [3] [4] gave two protocols later that were used for secure sequence outsourcing and algebraic computation outsourcing. Since these two protocols used burdened cryptography algorithm like homomorphic encryption [11]. Thus were not very successful for large problem set due to huge complexity. Based on above concept, Hohenberger [2] defined secure outsourcing protocol of modular exponentiation, which was taken to be a public key cryptography method that was very expensive.

Latest, Atallah [8] et al. presented a safe protocol based on secret key concept for secure outsourcing that used matrix multiplication [12]. This mechanism performed very well due to assumption of only one server and computation effectiveness. The only lacking point is lot of overhead because of message passing. Concluding, these methods are still not efficient enough for secure LP outsourcing computation.

Safe multiparty working was given by Yao [6]. Two or more parties are allowed to execute functions for obtaining result along with preserving their input from each other. Result is computed along with hiding the input from both the parties individually. Basic SMC is efficient, Du and Atallah et al. gave customized solution under SMC context for problem such as scientific computation, sequence comparison, statistical analysis etc. [13]. Though applying these concepts directly to the cloud is problematic. The computational power of customer and cloud was not similar which could not be handled effectively, which is avoided in the given design by shifting all computational load to cloud only. The other problem is security asymmetry because no party alone knows all problem input, leading to difficulty in result validation.

In SMC, Li and Atallah [14] gave a solution to the participating parties to apply additive split of constraint matrix along with few cryptographic techniques that are executed in each step of simplex algorithm. The above method does show practical performance for big size problem and does not guarantee optimal solution. With the same method, Toft [15] gave a secret key sharing secure simplex algorithm that had less complexity than other protocols. In [16], Vaidya formulated a new improved simplex algorithm that worked on safe scalar product and protocol comparisons. Lately, Catrina et al. [17] gave a safe multiparty LP using fixed point arithmetic. Some other works are of Du [18] and Vaidya [19] who studies distinguished approaches of matrix based transformation to look inti privacy preserving linear programming. Later, Bednarz et al. [20] proved Du’s and Vaidya’s approach infeasible and proposed to use permutation matrices. Recently, Mangasarian gave two privacy protecting methods of linear programming on vertical [21] and horizontal divided [22] constraints matrix. Although, many techniques were proposed but all had computation asymmetry issues.

Cloud computing is not a very trustworthy platform. It may behave unfaithfully during computation which may lead to incorrect computation of result without the knowledge of the customer. Detecting this is not an easy task that when the data is being modified in cloud which results in incorrect computation outsourcing. Verifiable computation delegation has found huge interest in theoretical computer science communities where weak customers can find out the correctness of computational result with the help of powerful but not trusted servers with the use of very less resources. Some of latest results and outcome is specified by Glodwasser et al. [23]. Golle et al. [24], to defeat the untrusted servers presented the idea to append pre-calculated results along with the computation. In [25], Szada et al. further worked on ringer scheme to defeat servers that cannot be trusted. In [26] Du. Et al. gave a mechanism for grid computing to find the cheating done in outsourcing computation. Based on Merkle tree the servers gives a commitment on the result computed by it. This commitment is then used by the customer followed by a sampling technique to do result verification.

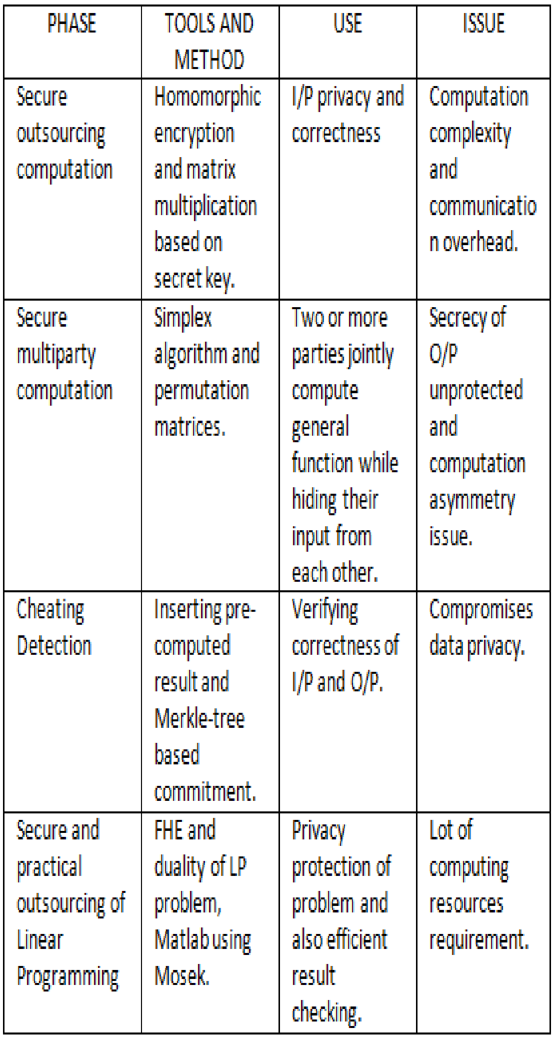
The above schemes looks into data and the computed result by it that is prohibited in cloud computing for security and safety of data. Thus it becomes tough task to provide result verification as well as input/output privacy. The introduction of concept of duality of LP problem efficiently performs the result validation, appending some overhead on customer server as well as cloud server.

Cong Wang [9], recently, gave an efficient and feasible method for securely outsourcing linear programming that will protect input/output and also find cheating servers. The data that are outsourced contains very insecure information such as medical history, financial details, research related works etc. To protect these important data and ensure its confidentiality it is encrypted before being outsourced to the cloud for computation. On the other hand, the details of computation is not transparent to user so there exists chances of cloud to behave unfaithfully and produce wrong output. Fully homomorphism encryption (FHE) scheme, has been shown feasible in theory for secure computation outsourcing

Computation outsourcing involves two different parts, cloud customer and cloud server. Cloud customer outsources LP problems to cloud server for computation. The cloud server has huge computing resources such as memory, storage and processing power. The customer sends its LP problem to CS after encrypting it with a secret key. The CS then computes the solution with the help of public LP solver running on the cloud and also produces a correctness proof. The customer on receiving the result verifies the result with the appended proof and then decrypt the result. The algorithm [27] is as follows:

- KeyGen(1^k) → {K}. It generates secret key K as an output on taking input the parameter k. This key K is used by the customer to perform encryption.
- ProbEnc(K,ϕ) → {Φ_k}. This step functions to encrypt the input, tuple ϕ into Φ_k, using the secret key K.
- ProofGen(Φ_K) → {y,Γ}. This algorithm provides solution of the LP problem $\Phi_K$to give the output or result y and proof Γ.
- ResultDec(K,ϕ,y,Γ) → {x,⊥}. Later the algorithm checks either x or y with the given proof Γ. The x is obtained by decrypting the output y with the help of secret key K. The output ⊥ is returned if correctness of output is not proved, that means the cloud has been compromised.

Table 1: Comparison between different mechanisms of secure outsourcing in cloud computing.



PHASE	TOOLS AND METHOD	USE	ISSUE
Secure outsourcing computation	Homomorphic encryption and matrix multiplication based on secret key.	I/P privacy and correctness	Computation complexity and communication overhead.
Secure multiparty computation	Simplex algorithm and permutation matrices.	Two or more parties jointly compute general function while hiding their input from each other.	Secrecy of O/P unprotected and computation asymmetry issue.
Cheating Detection	Inserting pre-computed result and Merkle-tree based commitment.	Verifying correctness of I/P and O/P.	Compromises data privacy.
Secure and practical outsourcing of Linear Programming	FHE and duality of LP problem, Matlab using Mosek.	Privacy protection of problem and also efficient result checking.	Lot of computing resources requirement.

III. PERFORMANCE OVERVIEW

With respect to the mechanism of LP, computation on side of customer consist of three algorithm such as KeyGen, ProbEnc and ResultDec. The complexity or overhead of computation is of generation of key, encryption operation and verification of result. The KeyGen and ResultDec algorithm consist of generation of random matrix along with multiplication of vector-vector and matrix vector. O(n^2) is the complexity of these two methods. The maximum time is consumed by matrix-matrix multiplication in ProbEnc algorithm. In cubic time method is used for matrix multiplication with the complexity of O(n^3). Other efficient methods are Strassen's algorithm [28] and Coppersmith Winograd algorithm [29] having complexity of O($n^{2.81}$) and O($n^{2.376}$) respectively.

The cloud server has to compute ProofGen algorithm that consist of solving LP problem_K that has been encrypted by the customer and computing the proof of result. If the problem_K is of normal case then the encrypted LP problem_K is solved with duality theorem to find optimal solution as the proof of result. The result proof is given in LP solving problem, thus no extra computation is required. In other case, an extra auxiliary LP problem_K does not has optimal solution. The LP is always computed at starting to find out the practical solution, thus it incurs an extra overhead.

Therefore in most of the cases, the complexity of computation is similar i.e. O(n^3) [30], same as in case of normal LP problem. Therefore, the more computation is performed on cloud which provides customer huge computation savings.

IV. ADVANTAGES AND DISADVANTAGES

One of the most important advantage is computational resources, the customer enjoys resources of cloud server by outsourcing the problem for computation. This saves capital investment of customer in hardware and software. It provides feature of correctness and soundness as the mechanism decrypts the output and verifies the result. Checks that if cloud has performed unfaithfully. Computing original LP by itself is more than the computation performed by customer. The computation overhead on CS is in the comparable time complexity of other practical algorithm of LP problems.

The $t_{original}$ /t_{cloud} [27], cloud efficiency, representing total overhead of the computation provides more than 30x savings.

Two different entities are involved in computation outsourcing architecture, one is customer cloud and the other is cloud server (CS) [9] [27]. The cloud customer has a very huge amount of sensitive and costly LP problems for being computed and outsourced and the cloud server has enough computing resources that provide computing services like public LP solvers.

V. CONCLUSION

Cloud computing has been proved to provide a lot of computation resources at less expenses. It provides user with limited resources to outsource their work or problem on cloud for computation which has ample amount of resources such as processing power, storage, bandwidth etc. Although, cloud provides too many benefits but security is a primary concern. The customer should be able to trust the cloud for their sensitive and confidential data being computed. Considering cloud as not a secure platform, a mechanism must be designed that not only protects user data but also ensures that result being computed is correct and verified.

This paper investigates about secure outsourcing and computation of LP problem. To attain efficiency LP problem is decomposed into public LP solvers. These solvers run on cloud. The resulting flexibility provides to find significant security and efficiency trade off with help of higher level abstraction of LP computation than the general circuit level. The transformation of LP problem in set of matrices and vector provides to apply privacy preserving technique that helps to change initial LP problem to an auxiliary one along with preserving insecure input/output operation. For verifying the computed output, fundamental duality theorem of linear programming is explored and necessary condition ae derived that should satisfy the results correctness. Tending-to-zero overhead is done by the mechanism on whole. The main function of this mechanism is that, along with security of data it also gives means to validate the data and the result.

REFERENCES

[1]. 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.

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

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

[4]. D. Benjamin and M.J. Atallah, “Private and cheating-free outsourcing of algebraic computation,” in Proc. Int. Conf. Privacy, Secur., Trust, 2008, pp. 240-245.

[5]. 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.

[6]. A. C.-C. Yao, “Protocols for secure computations (extended abstract),” in Proc. of FOCS, 1982, pp. 160–164.

[7]. C. Gentry, “Fully homomorphic encryption using ideal lattices,” in Proc of STOC, 2009, pp. 169–178.

[8]. M. Atallah and K. Frikken, “Securely outsourcing linear algebra computations,” in Proc. of ASIACCS, 2010, pp. 48–59.

[9]. Cong Wang, Kui Ren, and Jia Wang, “Secure and Practical Outsourcing of Linear Programming in Cloud Computing”, IEEE, 2011, pp. 820-821.

[10]. D. Luenberger and Y. Ye, Linear and Nonlinear Programming, 3rd ed. Springer, 2008.

[11]. P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in Proc. 17th Int. Conf. Theory Appl. Cryptographic Tech., 1999, pp. 223–238.

[12]. A. Shamir, “How to share a secret,” Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.

[13]. W.Du and M. J. Atallah, “Secure multi-party computation problems and their applications: A review and open problems,” in Proc. New Secur. Paradigms Workshop, 2001, pp. 13–22.

[14]. J. Li and M. J. Atallah, “Secure and private collaborative linear programming,” in Proc. Int. Conf. Collaborative Comput., 2006, pp. 1–8.

[15]. T. Toft, “Solving linear programs using multiparty computation,” in Proc. 13th Int. Conf. Financial Cryptography Data Security, 2009, pp. 90–107.

[16]. J. Vaidya, “A secure revised simplex algorithm for privacy-preserving linear programming,” in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl., 2009, pp. 347–354.

[17]. O. Catrina and S. De Hoogh, “Secure multiparty linear programming using fixed-point arithmetic,” in Proc. 15th Eur. Conf. Res. Comput. Security, 2010, pp. 134–150.

[18]. W. Du, “A study of several specific secure two-party computation problems,” Ph.D. dissertation, Comput. Sci. Dept., Purdue Univ., West Lafayette, IN, USA, 2001.

[19]. J. Vaidya, “Privacy-preserving linear programming,” in Proc. 24th ACM Symp. Appl. Comput., 2009, pp. 2002–2007.

[20]. A. Bednarz, N. Bean, and M. Roughan, “Hiccups on the road to privacy-preserving linear programming,” in Proc. ACM Workshop Privacy Electron. Soc., 2009, pp. 117–120.

[21]. O. L. Mangasarian, “Privacy-preserving linear programming,” Optim. Lett., vol. 5, pp. 165–172, 2011.

[22]. O. L. Mangasarian, “Privacy-preserving horizontally partitioned linear programs,” Optim. Lett., vol. 6, no. 3, pp. 431–436, 2012.

[23]. S. Goldwasser, Y. Kalai, and G. Rothblum, “Delegating computation: interactive proofs for muggles,” in Proc. 40th Annu. ACM Symp. Theory Comput., 2008, pp. 113–122.

[24]. P. Golle and I. Mironov, “Uncheatable distributed computations,” in Proc. Conf. Topics Cryptol.: The Cryptographer’s Track RSA, 2001, pp. 425–440.

[25]. D. Szajda, B. G. Lawson, and J. Owen, “Hardening functions for large scale distributed computations,” in Proc. IEEE Symp. Secur. Privacy, 2003, pp. 216–224.

[26]. D. Szajda, B. G. Lawson, and J. Owen, “Hardening functions for large scale distributed computations,” in Proc. IEEE Symp. Secur. Privacy, 2003, pp. 216–224.

[27]. Cong Wang, Kui Ren, and Jia Wang, “Secure Optimization Computation Outsourcing in Cloud Computing: A Case Study of Linear Programming”, in IEEE transactions on computers, vol. 65, No. 1, January 2016, pp. 219.

[28]. V. Strassen, “Gaussian elimination is not optimal,” Numer. Math., vol. 13, pp. 354–356, 1969.

[29]. D. Coppersmith and S. Winograd, “Matrix multiplication via arithmetic progressions,” in Proc. 19th Annu. ACM Symp. Theory Comput., 1987, pp. 1–6.

[30]. D. Luenberger and Y. Ye, Linear and Nonlinear Programming, 3rd ed. New York, NY, USA: Springer, 2008.