Indian J.Sci.Res. 17(2): 575-579, 2018

ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

ENCRYPTING CONFIDENTIAL FILES BEFORE UPLOAD TO CLOUD USING LINEAR METHOD FOR ENHANCED SECURITY

[1]Kavita Selkery, [2]M.Saravanan
[1,2] Department of Computer Science and Engineering, Aurora's Technological & Research Institute, Hyderabad, Telangana.

Abstract- Cloud computing in today's era is a cheaper and secure way to provide security to one's personal information. It is cheaper in the sense, that it is used in a pay-per-user manner, and is secure in a way, as only the authorized customer/owner of the information will be able to access it. Despite of this, data stored in Cloud Server (CS) is prone to threats, like, some software bugs, a hardware failure of/on CS or the cloud itself tempted to see the user uploaded file in cloud. Suppose, an organization has uploaded this year's financial report or their stocks information in share market etc., on CS, which he/she needs not to get compromised in any case. To ensure that, many encryption algorithms have been proposed/used in the past like Fully Homomorphic Encryption (FHE), RSA, etc. But those are also insufficient to ensure full security of data in CS, as the ciphertext has the form more or less similar to the plaintext. So this paper investigates the idea of encrypting user's confidential data more securely and in an optimized form, by providing enhanced security, by encrypting the data into ciphertext using the conventional RSA algorithm, along with the mathematical approach of Linear Programming (LP) method. In addition to ensuring highly encrypted data in the cloud, we explored LP methodology to verify, that, downloaded file is same as the optimized uploaded file, thus, ensuring not modified by an external entity.

keywords-Confidential Data, Cloud Computing, Linear Programming, Encryption.

I. Introduction

Cloud provides a robust platform along with its powerful computing power to the public for their confidential data to be stored with minimum cost. One of the main usages provided by the cloud is its computation outsourcing. With outsourcing, now customers need not worry about their hardware devices (including but not limited to RAM sizes, Memory requirements, etc.), requiring abundant space for their work-related resources/software. Instead, they can use the large pool of Computing resources/space/memory provided by cloud in an affordably pay-per-use manner. Also, for data storage purpose cloud is considered as one of the safest places as it provides authorization access to its users. Thus we can say that cloud computing is the cheaper and secure way to provide security to a customer's personal information.

It is cheaper in the sense that it used in a pay-per-user manner, i.e., a customer has to pay only for space, depending on the amount of data he/she wants to store in the cloud. And it is secure in a way, as only the customer/owner of the information will be able to access it, as he/she will only be having the authorized access to their information. But, despite of these merits, verified computing to the commercially available public cloud is also generating challenges and security concerns towards this, which is ultimately leading to troubling customers' as they don't have the power to ensure if their relevant and highly important data has been moved to

cloud without any security threat[3]. As the verified/subcontracted computation/space in clouds often carry huge personal and sensitive data of ones, such as the organization's yearly/quarterly/monthly financial reports, any institutions research data, or an individual's medical data, etc. To ensure the security of data from any unauthorized access, it has to be encrypted first before transferring to cloud[3]. And also while downloading back to its system customer needs to ensure security so as not be modified by any external entity.

Although, some encryption techniques are available, to ensure security, by inhibiting cloud from doing any purposeful manipulations on the hidden plaintext [4], thereby making the verification over ciphertext a big challenge. On the contrary, the internal operating details of the cloud are not available to customers [3]. As a result of which, Cloud Server (CS) purposefully may try to go unfaithful and will thus return wrong results which will not match with the original one.

Also, apart from clouds, dishonest behavior, more possible threats could be software bugs, hardware failure. Thus, it is understood that cloud is radically insecure from the customers point of view. Without ensuring a proper and robust secure process for transfer of data from customer's local systems to CS and the verified copy back from cloud to customer's owned machine, it is not advisable to store data in cloud just by looking at its affordable prices or savings and its easy resource availability. Also, while ensuring security of data, one more concern arises thereby adding further to responsibility of cloud, which is to ensure that customers need not to be involved in the manipulations/operations required to encrypt their data to provide security in cloud. As carrying out the operations for

[1]**Corresponding Author**

encryption may involve huge calculations and a large number of computations, which will only add to customers concern. Contrarily, then why would a customer look after cloud for the storage of their utmost important data? Many cryptography algorithms have been introduced and are currently used by cloud service providers to provide security to users data and also the number of computer science associations have made steady advances in "secure outsourcing expensive computations." (e.g. [5], [6], [7], [8], [9], [10]). Depending on mechanisms of Yao's garbled circuits [11] and Gentry's revolutionalized work on Fully Homomorphic Encryption (FHE) scheme [12], a verified result of secure encrypted transfer of data has been possible theoretically, in which the calculation is done using an encrypted combinational boolean circuits that facilitates to be calculated with encrypted private user provided inputs. Although, applying this technique to daily calculations is just not only impossible, due to extremely high complexity of FHE operation and the large sizes of circuits or keys involved to formulate the plaintext and the ciphertext thereby increasing the size of ciphertexts. This will eventually lead to buy more space in cloud, and thus customer has to pay more thereby diluting the idea of efficient cloud concept. Thus, due to the lack of effective solutions provided by these mechanisms, it has been a continuous motivation for most of the aspiring researchers to formulate an efficient way of concept or algorithm, for the successful transfer of data in cloud in a secure and an optimized way.

However in addition to above mechanisms, number of other ingenious designs for secure outsourcing of data using sequence comparisons and matrix multiplication, etc. have been contemplated, but that is also difficult to implement efficiently for practically large problems.

Implementing these cryptographic calculations on cloud side will be result in heavy computations for cloud [7], [8], adding to the complexities involved in communication[10] with the customer regarding the authorization information. Thus, still, the practically efficient and feasible solutions for secure and optimized encrypted outsourcing in cloud is still lacking. Considering, probable engineering computing and secure optimizing burdens, in this paper, we present the idea of fundamentally adapted ways for protected outsourcing of linear programming (LP) estimations.

LP is an analytical and numerical mechanism which takes into account the first derived results of the conventional algorithms that should be optimized and is necessary to achieve engineering optimization. Since, LP computations needs considerable amount of computation power and it consistently deals with confidential data, like a customer's annual financial report or his stocks information in share market etc., therefore looking into the problem definition of application-specific we state to specifically disintegrate the LP mechanism for utilizing cloud storage, into public LP solvers which are executing on the cloud and secret LP variables retained by customer. The compliance of such a disintegration permits us to examine more into LP methodology than the normal circuit model for the feasible adaptability.

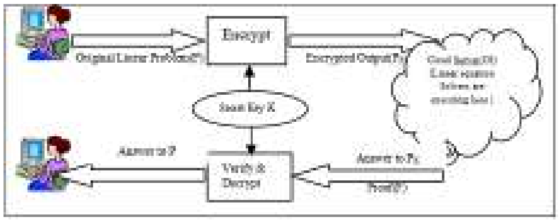


Fig 1. Linear mechanism for uploading encrypted output in cloud and receiving a verified answer from cloud to ensure no loss of data and unmodified data in cloud.

This LP mechanism to solve problem can be described as shown in the Fig. 1. To be more specific, we first perform calculation on the private data retained by the user for LP problem as a set of matrices or vectors.

One important outcome, of this problem transformation methodology, is that existing algorithms and devices for LP solvers can be reused by CS. To verify and validate the output, we use the fact that, the output is from CS, and further applying reverse the LP mechanism to its output first will not only be efficient but will also induce negligible extra effort on both sides, i.e., user and CS. Using accurate established results, user will then be able to transform the desired data back to its original form using the secret key.

II. Problem Definition

Our verified information transfer flow is described using Fig.1: the user having large data or technically our LP problem (P) to be solved. Since, a customer is having limitations performing huge, costly, and complex calculations on his machine, about processing capacity, RAM size, and storage, etc., thus, the customer seeks out help from CS for solving his LP problem and makes use of its robust mechanism for calculations in pay-per-use manner.

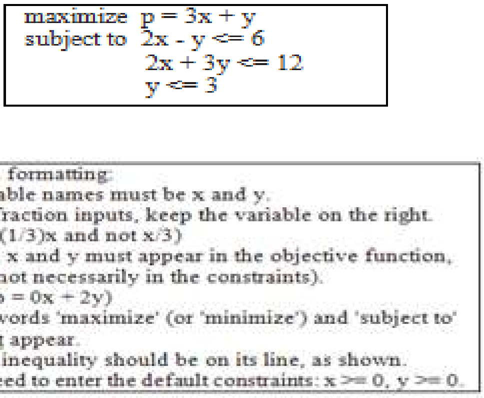
To ensure security, customer does not send the original LP(P) directly to CS, but first using his secret key K maps P into some ciphertext P_K and then passes P_K to CS. CS then uses its public LP program executing on it, to generate the output of PK and its proof F, for verifying its accuracy, but CS itself does not learn anything from the original sensitive data.

Once the customer gets the output of encrypted PK, he has first to verify that using the added proof F. In case the result is as expected then customer will make use of his secret key K to again map the resultant into the expected solution to his original problem P.

III. Linear Programming Overview

LP is a way to maximize or minimize a defined quanti an optimized way. This approach involves defining a problem as a set of linear equations and then applying constraints in a situation by a system of inequalities, and thus finds how these applied constraints affect certain quantities in an optimal way. Thus a LP problem(LP) can be represented as follows:

Minimize ctx subject to Ax=b, provided x>=0. (1)



maximize p = 3x + y
subject to 2x - y <= 6
2x + 3y <= 12
y <= 3

Notes on formatting:
(1) Variable names must be x and y.
(2) For fraction inputs, keep the variable on the right.
(eg. (1/3)x and not x/3)
(3) Both x and y must appear in the objective function,
(but not necessarily in the constraints).
(eg. p = 0x + 2y)
(4) The words 'maximize' (or 'minimize') and 'subject to' must appear.
(5) Each inequality should be on its line, as shown.
(6) No need to enter the default constraints: x >= 0, y >= 0.

Fig 2. Objective function maximize (p), subjecting to the conditions specified as the linear inequalities which must satisfy.

In above equation(1), x,c,b are column vectors and A is a 2-dimensional matrix.

We can rewrite above equation in a more generalized way as follows:

Minimize ctx subjectto Ax=b, provided Bx>=0. (2)

Inequation(2), B is a square matrix, used to ensure positive values as Bx. We will get equation(1) if B is an identity matrix.

IV. Proposed Methodology Overview

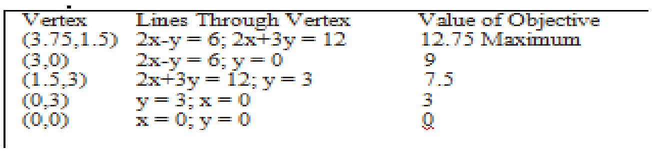
Here we have explained our solution to original LP problem (P). Since, we specifically disintegrate the LP mechanism for utilizing cloud storage, into public LP solvers which are executing on the cloud and secret LP variables retained by customer. The compliance of such disintegration permits us to examine more into LP methodology than the normal circuit model for the feasible adaptability.

To be more specific, we first perform calculation on the private data retained by the user for LP problem as a set of matrices or vectors.

One important outcome, of this problem transformation methodology, is that existing algorithms and devices for LP solvers can be reused by CS. To verify and validate the output, we use the fact that, the output is from CS, and further applying reverse the LP mechanism to its output first will not only be efficient but will also induce negligible extra effort on both sides, i.e., user and CS. Using accurate established results, user will then be able to transform the desired data back to its original form using the secret key.

Our implementation for this mechanism is as illustrated in above Fig. 2. Here, as we can see the linear inequalities, we require along with the maximizing objective function (which is for maximizing security), taking into consideration the necessary conditions to be satisfied.

For solving customer specific problem, they have to provide the required minimum and maximum x and y variables, which are private and secret parameters known only by user/customer. Thus, in that way the answer generated after solving those values (shown in Fig.3 the inequalities and equations after entering some values as experimental results), by linear method will be unique for each and every file and making it impossible for cloud/outsider to guess the lp key generated during this process.



Vertex	Lines Through Vertex	Value of Objective
(3.75,1.5)	2x-y = 6; 2x+3y = 12	12.75 Maximum
(3,0)	2x-y = 6; y = 0	9
(1.5,3)	2x+3y = 12; y = 3	7.5
(0,3)	y = 3; x = 0	3
(0,0)	x = 0; y = 0	0

Fig 3. Experimental results showing equations for solving the original Linear problem.

A. Mechanism For Secure LP Outsourcing

Our complete LP formulation methodology is based on basically four algorithms. The program on CS running generally can be stated by algorithm for 1. Generating Proof (F). And the programs executing on customer side can be stated by algorithms for 2. Generating Secret Key (K), 3. Encrypting data or LP problem (P) using K to get PK, and finally, for 4. Generating the desired answer (P) back along with the proof (F) for customer to verify the accuracy of original and the ciphertext data stored in cloud.

In this way, this design ensures that a same secret key K will never used for two separate problems/data files.Using this mechanism, we have identified the performance using various parameters as Encryption Time, Decryption Time, File Access Time depending on the size of file, as shown in the table “Table 1”. negligible overhead on cloud and customer side too.

Table 1

File Size(KB)	Encryption Time (Secs)	Decryption Time (Secs)	File Access time in Cloud

1 to 30	2 to 4	1 to 2	1 to 2
30 to 80	3 to 7	2 to 4	1 to 3
80 to 200	4 to 9	2 to 5	2 to 5
250 to 550	4 to 9	3 to 7	2 to 5
550 to 780	5 to 11	6 to 10	5 to 13

Table 1. Various evaluated parameters based on our experimental results while using Linear approach for solving the problem, which shows a decent minimization in the time required for different activities performed.

V. Conclusion andFuture work

In this paper, we explored the idea of LP methodology for transfer of encrypted confidential data of customer to cloud in a secure and optimized way, thereby ensuring the input/output privacy and efficiency. By specifically disintegrating the LP mechanism for utilizing cloud storage, into public LP solvers which are executing on the cloud and secret LP variables retained by customer. The compliance of such disintegration permits us to examine more into LP methodology than the normal circuit model for the feasible adaptability. To be more specific, we first perform calculation on the private data retained by the user for LP problem as a set of matrices or vectors. As it uses the variables secretly owned by customers only, it ensures that, it’s near to impossible for hackers or cloud itself to access the encrypted data and acquire the confidential information of customer. Also, this paper investigates the round trip verification theorem, by generating the proof for accurate results. It helps customers to validate, whether their encrypted data stored in cloud can be regenerated back to the original data using their secret key. Also implementing such mechanism incurs

A. Future Enhancements

Till now, we have discussed about the security of confidential data of customer stored in cloud using mathematical paradigm of LP mechanism. The data we have used so far in this was in the form of text file or word file. But, this can be enhanced further to provide security to files other than text files or documents, i.e., like image files and video files too.

To achieve this one can use the image encryption algorithms to achieve security of image file in cloud along with the linear methodology, and also to ensure that after decryption we will get the same file as the uploaded one, without being accessed or modified by an external entity.

References

[1] 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] 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.

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

[14] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, Introduction to Algorithms, 2nd Cambridge, MA, USA: MIT Press, 2008.

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

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

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

[19] 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.