Secure Computations Outsourcing of Mathematical Optimization and Linear Algebra Tasks: Survey

[1] Nedal M. Mohammed, [2] Santosh S. Lomte

[1,2]Department of Computer Science, Dr. Babasaheb Ambedkar Marathwada University, India.

[1]Department of Computer Science, Taiz University, Taiz, Yemen.

***Abstract*— One of a powerful application in the age of cloud computing is the computation outsourcing which makes cloud computing a very powerful computing paradigm, where the customers with limited computing resource and storage devices can outsource the sophisticated computation workloads into powerful service providers, and use the unlimited computing resources in a pay-per-use manner. Despite these benefits, the outsourcing paradigm also inevitably suffers from some new security challenges due to untrusted cloud servers. This paper covered the latest samples of recent advances in the secure computation outsourcing methods for optimization and linear algebra tasks and security challenges in outsourcing computation. We implemented studied samples schemas on the customer side laptop and using AWS compute domain elastic compute cloud (EC2) for the cloud side and use these implemented result for comparison between the studied schemes. We then provide a list of open challenges in the area.**

***Keywords*— *Secure scientific computation outsourcing; Verifiable computing linear algebra; Secure optemaization problem* .**

I. INTRODUCTION

Cloud computing [1] emerged as a new computing model for complex systems with massive-scale services sharing among numerous users. Outsourcing is the powerful advantage of cloud computing, it makes cloud computing a very powerful computing paradigm, where the customers with limited resources and constrained devices can outsource the complex computation workloads into untrusted cloud servers and enjoy the unlimited computing resources in a pay-per-use manner. Despite the tremendous benefits, because customers and cloud are not necessarily in the same trusted domain brings many security concerns and challenges toward this promising computation outsourcing model [2]. First, customer's data that are processed and generated during the computation in cloud are often sensitive in nature, such as business financial records, proprietary research data, and personally identifiable health information, etc. While applying ordinary encryption techniques to these sensitive information before outsourcing could be one way to combat the security concern. It also makes the task of computation over encrypted data in general a very difficult problem [3]. Second, since the operational details inside the cloud are not transparent enough to customers [2], no guarantee is provided on the quality of the computed results from the cloud. The theoretical computer science community has devoted considerable attention to the problem of how to securely outsource different kinds of expensive computations. Generally, we can view any mathematical optimization and linear algebra computation task as a function $F : D \rightarrow M$ on a domain D such that $F(D) \subseteq M$. Given any $x \in D$, the goal is to compute $F(x)$. In the outsourcing paradigm, an honest but resources-contained client C wants to delegate the computation task $F(x)$ to a cloud server S that is not fully trusted by C. Firstly, C may outsource the encoding of F and x to C (that is, the information about F and x should be kept a secret to S in some scenarios). Secondly, C returns the computation result based on the input (note that the output is not $F(x)$). Finally, the client C efficiently verifies that the output provided by S is valid and then computes the final result $F(x)$ by himself. This paper mainly discusses the literature that focuses on issues of secure outsourcing mathematical optimization and linear algebra computation task. The paper is organized as follows. In Section 2, we introduce some secure challenges in outsourcing computation. In Section 3 we discuss some of related work to secure outsourcing computation with summary of comparison results. Finally, Section 4 is the conclusion of the study and future directions.

 DOI : 10.18231/2454-9150.2018.0860

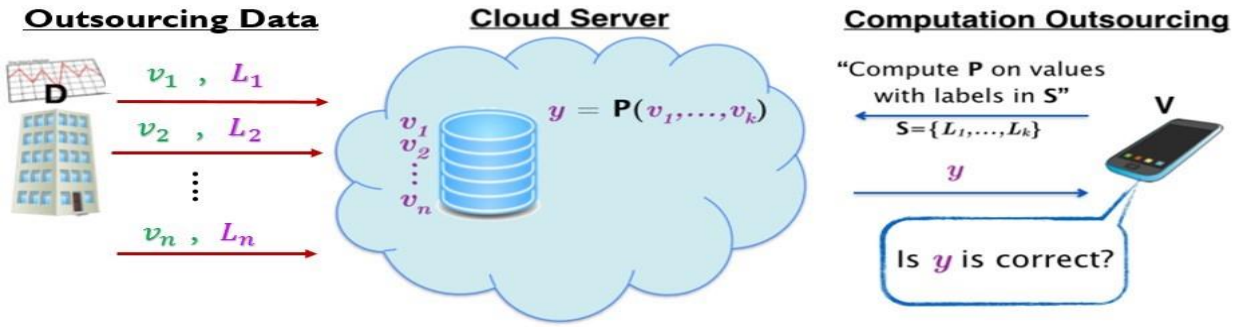

Fig 1. Verifiable Computation on Outsourced Data

II. SECURE CHALLENGES IN OUTSOURCING COMPUTATION

The outsourcing of expensive computations to untrusted cloud servers are getting more and more attentions in the scientific community. However, on the other hand, the shift from local to remote storage and loss of control over the outsourcing computation raises new challenges. Some new security challenges are:

- The **secrecy** of the outsourcing computation: The cloud servers should not learn anything about what they are actually computing (secret input & output result).
- The **checkability** of the outsourcing computation: The semi-trusted cloud servers may return some invalid results so that the client should have the ability to detect any failures if the cloud servers misbehave.
- The **efficiency** of the outsourcing computation. That is, the outsourcing protocols should not require multiple rounds of interactions between the client and servers.

III. RELATED WORK

Many works have been done in the framework of secure outsourcing within the scope of many research areas. Gennaro et al. [5] first formalized the definition for secure outsourcing computation which consists some verifiable computation scheme (KeyGen, ProbGen, Compute, Verify) and presented a milestone theoretic framework for secure outsourcing arbitrary computation functions. The framework mainly uses two building blocks of garbled circuit [6] and fully homomorphic encryption [7]. Atallah et al. [8] presented a framework for secure outsourcing of scientific computations such as matrix multiplications and quadrature. Gennaro et al., Golle et al. and Hohenberger et al. [5, 9, 10] introduce four kinds of adversarial models for secure outsourcing computation. The secrecy can be achieved by means of special encryption or disguise, but how it can efficiently verify the computation results. For that there are three approaches: The first one is suitable for the verification itself which is not involved in any expensive computations, i.e. inversion of one-way function class of outsourcing computations [11, 9], the client can directly verify the result since the verification is just equivalent to compute the one-way functions. The second approach is that the client uses multiple servers to achieve verifiability [10]. That is, the client sends the random test query to multiple servers and it accepts only if all the servers outputs give the same result. Trivially, the approach can only ensure the client to detect the error with probability absolutely less than 1. The last approach is based on one malicious server and might leverage some proof systems [4]. Obviously, an essential requirement is that the client must verify the proofs efficiently. Xiang et al. [12] they proposed a verification scheme involving approximate Karush-Kuhn-Tucker (KKT) conditions with the ε−KKT point. This scheme does not involve any cryptographic tools and thus is efficient and effective. The framework for secure outsourcing of scientific computations first analyzed and presented by Atallah et al. [8]. Benjamin and Atallah [13] proposed some protocols for secure outsourcing linear algebra computations. However, it required the expensive operations of homomorphic encryptions. The efficient mechanism was proposed by Wang et al.[14] for secure outsourcing computations of linear programming. However, the solution requires (nρ) for some $2 < \rho \leq 3$ time computational. Some other works [15] also used Shamir's secret sharing to perform homomorphic computations over the cloud. Trivially, the protocols based on secret sharing require at least two non-colluding servers. Seitkulov [16] proposed other ways of verified disguise that solve abstract equations, Cauchy with secret parameters and boundary value problems of secret boundary condition issues. Recently, Wang et al.[17] proposed a secure outsourcing mechanism for solving large-scale systems of linear equations based on the iterative methods. Nie et al. [18] proposed an efficient secure outsourcing algorithm using sparse matrix for large-scale systems of linear programming, this algorithm only requires O(n2) time computational. Also, the client C can detect the misbehavior of cloud server S with probability 1 under the computational complexity of O(n). Zhou and Li.[19] designed a protocol for computations outsourcing of large-scale quadratic programming to cloud, also developed techniques that enable the customer to protect the sensitive input/output information by transforming the original quadratic programming into some encrypted form, moreover used

 DOI : 10.18231/2454-9150.2018.0860

Karush-Kuhn-Tucker (KKT) conditions to verify the result. Salinas et al. [20] design a low complexity matrix transformation scheme that protects the private data in a quadratic programming, then they proposed algorithm to solve the transformed quadratic programming at the cloud.

Table 1. Summary of most important researches

S.no	Title	Remark	limitations
1	Li et al. [36].	This scheme is efficient and publicly verifiable it allows the clients to verify the correctness of returned results by using the public key. and it proved to be secure and correct.	Same matter in [24] because the computation result ought to belong to a polynomial size domain.
2	Li and Atallah [21].	Series of interactive cryptographic protocols collaboratively executed in each iteration step. *(Simplex Algorithm)*	Cannot be done for non-linear optimization problems.
3	Benjamin and Atallah [13].	Addressed the problem of secure outsourcing for widely applicable linear algebra computations.	The proposed protocol required the expensive operations of homomorphic encryptions.
4	Atallah and Frikken [22].	They improved protocols for linear equation and linear programming based on Shamir's secret sharing.	This schema requires multi-round interactions between the customer and cloud server and e protocols based on Secret sharing require at least two noncolluding servers.
5	Wang et al.[14]	Secure outsourcing of linear programming computation schema was proposed it based on the problem transformation.(More efficient)	The solution requires (n^{ρ}) for some $2 < \rho \leq 3$ time computational.(Problem-specific, less security)
6	Fiore and Gennaro[23]	Proposed an outsourced matrix multiplication scheme based on the pseudorandom functions (**PRF**). The client can verify the correctness of the result by using the secret key.	The client is required to precompute a tag for each column victor of the matrix which can be inefficient.
7	Wang et al. [17].	A secure outsourcing scheme based on the iterative methods was proposed for solving large-scale systems of linear equations.(More secure and general)	It would be impractical because it requires multi-round interactions between the customer and cloud server.(Inefficient)
8	Zhang and Safavi-Naini [5].	Proposed a matrix multiplication scheme based on multilinear maps and the property of prfs.	The scheme requires client computing a multitude of tags before outsourcing the computation which may degrade the efficiency.
9	Zhang J. et al. [25].	They Proposed efficient scheme for secure outsourcing of linear algebra based on fully homomorphic encryption.	This schema requires high computation.
10	Li D et al. [26].	They constructed a new efficient matrix encryption scheme. Then exploit this encryption scheme to develop an algorithm which can implement outsourcing storage and computation for large-scale linear equations in the semi-honest setting.	Computation of solve (*1.5knM + nM).*

 DOI : 10.18231/2454-9150.2018.0860

IV. SECURITY ANALYSIS, COMPARISON AND DISCUSSION

The large-scale problem-specific outsourcing, such as (linear equation system (LES), linear programming (LP), nonlinear programming (NLP) and QP (quadratic programming) outsourcing, usually use random affine mapping to transform the original computation problem to take on an encrypted form, which can then be outsourced to an untrusted public cloud for solving. When performing the affine-mapping, the most costly computation is the multiplication of matrices. We studied security treatment of secure computation outsourcing of above problems and analysis some proposed methods for matrices multiplication which they are used, we briefly summarize performance speed-up for different schemes in table 2, and categorize existing solutions of large-scale secure computation outsourcing by evaluated performance computational task and comparing the encryption/decryption or transformation overhead as well as task verification cost to computation overhead of performing the original task. Because of the original motivation of outsourcing large-scale computation, performance speed-up is a necessary requirement for outsourcing schemes. The customer side devices usually have limited physical memory and weak computing power. While the computation problems(LES, LP, NLP, QP) to be outsourced usually have very large inputs that are expressed in basic mathematical objects such as matrices. So in this paper, we experiment some algorithms(Atallah [38], Atallah [22], random matrix disguising (RMD) [14], fast matrix disguising(FMD) [37], and Benjain [13]) and compare between them according to memory requirement. It can be seen from Table 2 and Figure 2, for the majority of matrix dimensions (n) FMD algorithm runs faster than RMD and Atallah[38] algorithms. But FMD algorithm is slower than Atallah96 algorithm when the matrix dimension increases to ten thousand. This is because Atallah[38] algorithm generally consumes less memory(handle the matrix in physical memory), while FMD1(difference size of virtuel memory) algorithm begins to utilize virtual memory. However, when all the schemes begin to use virtual memory, FMD algorithm is still the fastest. And if we decrease the security level of the matrix dimension n, FMD algorithm will always outperform Atallah[38] algorithm. Atallah[22] and Benjain algorithms are two outsourcing methods. Suppose the outsourcing environments provide unlimited bandwidth and computing/memory resources, we only measure the time consumption on the customer side. It is clear that Atallah [22] algorithm and Benjain algorithm demand more memory than other methods and will exhaust physical memory when they try to disguise matrices whose dimensions are large.

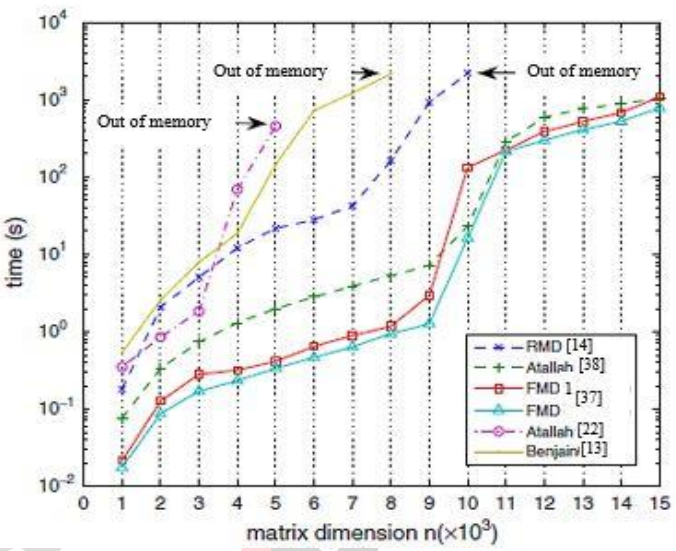

Figure 2. Comparison between [13],[14],[22],[37],[38] algorithms.

Table 2. Summary comparison of most important algorithm for outsourcing.

Algorithm	Task	Encryption Deception time	Task time	Verification time
Wang et al.[17]	System of linear equations	$O(n(i+n))$	$O(n^{\rho})$	$O(n^2)$
		$O(n(i+n))$		$O(ln^2)$
Chen et al.[27]		$O(n^2)$		$O(n^2)$
Chen et al.[28]		$O(\lambda n)$		$O(n^2)$
Benjamin and Atallah [13]	Matrix multiplication	$O(n^2)$	$O(n^{\rho})$	$O(n^2)$
Atallah and Frikken[22]		$O(t^2n^2)$	$O(tn^{\rho})$	$O(n^2)$
Lei et al.[29]		$O(mn+ns+ms)$	$O(msn)$	$O(msl)$
Mohassel [30]		$O(n^2)$	$O(n^{\rho})$	$O(n^2)$
Zhang and Blanton[31]		$O(mn+ns+ms)$	$O(msn)$	$O(ms)$
Fiore and Gennaro[23]		$O(n^2)$	$O(n^{\rho})$	$O(n^2)$
Lei et al.[32]	Matrix inversion	$O(n^2)$	$O(n^{\rho})$	$O(n^2)$

DOI : 10.18231/2454-9150.2018.0860

Duan et al.[33]	Nonnegative matrix factorization	$O(max(m,n)^2)$	$O(imnr)$	$O(mnr)$
Zhou and Li[34]	Matrix Eigen decomposition	$O(n^2)$	$O(ln^2)$	$\Omega(n^3)$
Zhou and Li[34]	Singular value decomposition	$O(n^2)$	$O(ln^2)$	$O(n^3)$
Lei et al.[35]	Matrix determinant	$O(n^2)$	$O(n^\rho)$	$O(ln^2)$

Table 2. Summarizes performance speed-up for different algorithms for computation outsourcing. For example, in some algorithms the transformation uses a random matrix for hiding the original data. Client's computation is dominated by several matrix additions and matrix-vector multiplications.

Notation used in Tables 1 and 2 :

n: The number of columns in the first non-square matrix.
m: The number of rows in the first non-square matrix.
s: The number of rows in the second non-square matrix.
t: Secret sharing threshold.
ρ: The power in the asymptotic complexity of matrix multiplication.
l: The number of iterations in the verification process.
i: The number of iterations needed in the computation.
λ: The upper bound on the number of non-zero elements in each matrix row.
r: Dimension parameter for matrix factorization.
p: The number of rows in the constraint matrix for optimization problems.

V. CONCLUSION AND FUTURE DIRECTIONS

The survey critically investigates different security frameworks proposed for the secure outsourcing computation. This paper presented the research related to secure outsourcing computation systems along with their weaknesses and drawbacks. Outsourcing computation is a fruitful and long-standing research topic in the academic community. With the development in this field, we believe that more and more researchers will focus on this interesting topic. In the following, we present our future directions in secure computation outsourcing.

- Design efficient algorithm which only requires one round of interaction between the server and the client to obtain
- Securely outsourcing the cryptographic operations by only using an untrusted server.
- Find some more efficient algorithms which can still achieve the strongest security notions.
- Efficient solution to solve this problem of detecting the misbehavior of an untrusted server in the multiple results of outsourcing computations by using some new primitives, such as verifiably searchable encryption.

REFERENCES

[1] Li H, Dai Y, Tian L, Yang H. Identity-based authentication for cloud computing. In Cloud computing. Springer. 2009;157–166.

[2] CSA Cloud Security Alliance, Security guidance for critical areas of focus in cloud computing. 2009. http://www.cloudsecurityalliance.org.

[3] Gentry C. Computing arbitrary functions of encrypted data. Comm. ACM. 2010; 53(3):97–105.

[4] Goldwasser S, Kalai Y, Rothblum G. Delegating computation: interactive proofs for muggles. Proceedings of the ACM Symposium on the theory of Computing (STOC). 2008;113–122.

[5] Gennaro R, Gentry C, Parno B. Non-interactive verifiable computing: Outsourcing computation to untrusted workers. Advances in Cryptology-CRYPTO, Springer. 2010;465–482.

[6] Yao A. Protocols for secure computations. Proceedings of the IEEE Symposium on Foundations of Computer Science. 1982;160–164. DOI: 10.1109/sfcs.1982.38. 8.

[7] Smart N, Vercauteren F. Fully homomorphic encryption with relatively small key and ciphertext sizes. Public Key Cryptography-PKC, Springer. 2010;420–443.

[8] Atallah M, Pantazopoulos K, Rice J, Spafford E. Secure outsourcing of scientific computations. Adv Comput. 2001; 54:216–272.

[9] Golle P, Mironov I. Uncheatable distributed computations. CT-RSA, Springer, LNCS 2020. 2001. 425–440.

[10] Hohenberger S, Lysyanskaya A. How to securely outsource cryptographic computations. theory of Cryptography, Springer, LNCS 3378. 2005;264–282.

[11] Blanton M. Improved conditional e-payments. Applied Cryptography and Network Security (ACNS), LNCS 5037, Springer. (2008;188–206.

[12] Xiang T., Zhang W., Zhong S., Yang J.: Verifiable outsourcing of constrained nonlinear programming by particle swarm optimization in cloud. Soft Computing. (2017),1–13.

[13] Benjamin D, Atallah M. Private and cheating-free outsourcing of algebraic computations. Proceedings of the 6th Annual Conference on Privacy, Security and Trust (PST). 2008;240–245.

 DOI : 10.18231/2454-9150.2018.0860

[14] Wang C, Ren K, Wang J. Secure and practical outsourcing of linear programming in cloud computing. Proceedings of the 30th IEEE International Conference on Computer Communications(INFOCOM).2011;820-828.

[15] Mohanty M, Ooi W, Atrey P. Scale me, crop me, know me not: Supporting scaling and cropping in secret image sharing. IEEE International Conference on Multimedia and Expo. 2013;1 – 6.

[16] Seitkulov Y. New methods of secure outsourcing of scientific computations. Springer Science+Business Media. J Supercomput. 2013; 65:469–482.

[17] Wang C, Ren K, Wang J, Wang Q. Harnessing the cloud for securely outsourcing largescale systems of linear equations. IEEE Transactions on Parallel Distribution Systems. (2013 ; 24(6):1172–1181.

[18] Nie H, Chen X, Li J, Liu J, Lou W. Efficient and verifiable algorithm for secure outsourcing of large-scale linear programming. In Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conference on IEEE. 2014;591–596.

[19] Zhou L, Li C. Outsourcing large-scale quadratic programming to a public cloud. IEEE Access. 2015; 3:2581–2589.

[20] Salinas S, Luo C, Liao W, Li P. Efficient secure outsourcing of large-scale quadratic programs. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security ACM. 2016;281–292.

[21] Li J, Atallah M. Secure and private collaborative linear programming. in Proc.of CollaborateCom,Nov. 2006;1-8.

[22] Atallah M, Frikken K. Securely outsourcing linear algebra computations. Proceedings of the 5th ACM Symposium on Information. Computer and Communications Security (ASIACCS). (2010); 48–59.

[23] Fiore D, Gennaro R. Publicly verifiable delegation of large polynomials and matrix computations, with applications. IBM Research, CCS'12. 2012;501–512.

[24] Zhang L, Safavi-Naini R. Private outsourcing of polynomial evaluation and matrix multiplication using multilinear maps. in Cryptology and Network Security. Springer. 2013;329–348.

[25] Zhang J, Zhu Y, Jin F. Practical and secure outsourcing of linear algebra in the cloud. In: 2013 International Conference on Advanced Cloud and Big Data; 2013. p. 81–7. ISBN 978-1-4799-3261-0. d

[26] Li D, Dong X, Cao Z, Wang H. Privacy-preserving large-scale systems of linear equations in outsourcing storage and computation. Science China Information Sciences. 61 (3) 2018, 032112:1–032112:9.

[27] Chen F, Xiang T, Yang Y. Privacy-preserving and verifiable protocols for scientific computation outsourcing to the cloud. J. Parallel and Distrib. Comput. 2014; 74(3):2141–2151.

[28] Chen X, Huang X, Li J, Ma J, Lou W, Wong D. New algorithms for secure outsourcing of large-scale systems of linear equations. Transactions on Information Forensics and Security. 2015; 10(1).

[29] Lei X, Liao X, Huang T, Heriniaina F. Achieving security, robust cheating resistance, and high-efficiency for outsourcing large matrix multiplication computation to a malicious cloud. Information Sciences. 2014; 280:205–217.

[30] Mohassel P. Efficient and Secure Delegation of Linear Algebra. IACR Cryptology ePrint Archive. 2011;605.

[31] Zhang Y, Blanton M. Efficient secure and verifiable outsourcing of matrix multiplications. In International Conference on Information Security. 2014;158–178.

[32] Lei X, Liao X, Huang T, Li H, Hu C. Outsourcing large matrix inversion computation to a public cloud. IEEE Transactions on Cloud Computing. 2013;1(1).

[33] Duan J, Zhou J, Li Y. Secure and verifiable outsourcing of nonnegative matrix factorization (NMF). In The 4th ACM Workshop on Information Hiding and Multimedia Security, ACM. 2016;63–68.

[34] Zhou L, Li C. Outsourcing eigen-decomposition and singular value decomposition of large matrix to a public cloud. IEEE Access. 2016; 4:869–879.

[35] Lei X, Liao X, Huang T, Li H. Cloud computing service: The case of large matrix determinant computation. IEEE Transactions on Services Computing. 2015; 8(5):688–700.

[36] Li P, Xu H, Hong J. Private outsourcing of polynomial functions. IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications. 2014;61–68.

[37] Yulong Wang and Yi Li An efficient and tunable matrix-disguising method toward privacy-preserving computation, Security Comm. Networks 2015; **8**:3099–3110.

[38] Atallah MJ, Pantazopoulos KN, Spafford EH. Secure outsourcing of some computations. Computer Science Technical Reports, 1996.

 DOI : 10.18231/2454-9150.2018.0860