International Journal of Engineering & Technology, 7 (3.27) (2018) 318-320

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Protected Data Using Hybrid Algorithm in Cloud

K. Kalaiselvi[1*], N. Jayashri[2], G. Saraswathi[3]

[1]*Associate Professor and Head, VISTAS, Chennai, India.*
[2]*Research Scholar, VISTAS, Chennai, India. E-mail:jayashrichandrasekar@yahoo.co.in*
[3]*PG Student, VISTAS, Chennai, India. E-mail:jabssaras@gmail.com*
**Corresponding author E-mail:kalairaghu.scs@velsuniv.ac.in*

Abstract

Cloud computing providing confidentiality over the insensitive data was the major issue related to security. It verifies the data owned by the server through linear computations. The proposed work enables security and efficiency using the cryptographic techniques of hybrid algorithms, securing the sensitive information that is present in the cloud. In the hybrid algorithm, it is the combination of problem encryption, key generation, result decryption and proof generation. It also validates the results which are being computed and also provides end-to-end confidentiality over the data to both the end user. The uses of hybrid algorithm results in a random key generation, encrypt/decrypt, and validate the satisfied results. This will provide a low cost to both server and client.

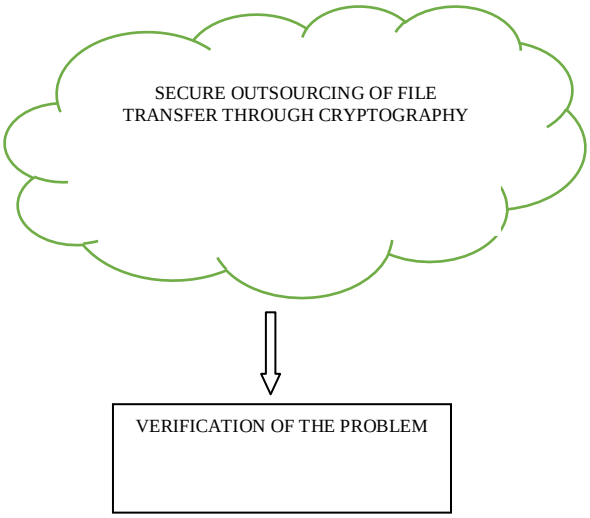
Keywords: *Hybrid algorithms, secure outsourcing, result decryption, problem encryption, key generation, proof generation.*

1. Introduction

Cloud Computing refers to the outsourcing service by other companies and service providers over the Internet. Cloud Computing is easily manageable. It provides easy access to the resources and available on-demand and provides 'pay-per-use' basis. Cloud is a technology where businesses store the confidential data. It acts as an endless pool for storing a large number of data. Cryptography maintains the privacy of data. It is a method of storing and transmitting data in a particular form so that the end user can read and process it. It keeps the information safe and secure. Encryption is the process of transforming information into an encrypted format to prevent unauthorized access. The process of decoding involves data that has been encrypted and it is transformed back into an original text format. It requires a secret key or password.

Linear Programming involves a practical method of solving the allocation of resources with the use of some linear functions in which the variables are restrained to the constraints. Linear programming involves basic linear problem and nonlinear programming also. Nonlinear programming includes at least one nonlinear function which refers to the objective function along with the constraints. It achieves the desired result at minimum cost and risk.

Vogel's approximation method is used for nonlinear programming. It is used for optimizing transportation cost and thus provides a feasible solution to an allocated problem. Regarding the basic linear solution, simplex and dual simplex method have been used. The dual simplex method provides an alternative solution to the linear problem used along with the algorithms.



2. Proposed Work

This proposed scheme represents security over the insensitive information that is in the cloud by using the cryptography technique and also maintains the efficiency of verification done through linear and nonlinear programming method for checking the end results.

Overview of the Framework

Security in the cloud can be obtained by applying the encryption and decryption along with the generation of the secret key through the cloud and also both linear and nonlinear programming disintegrations on the private data of the client for verification of files from the server. This technique makes the client to secretly transform the original problem into a random solution to achieve the secure outsourcing. Thus, it provides end-to-end

confidentiality between the client and server by guaranteeing either low or no cost to clients as well as servers.

Method Overview

More information at higher levels in the cloud platform makes the security concern out of range. The user needs a secure verification of data before and after the encryption and decryption so that no third party can act as an intruder and verify the file. Thus the factor uniqueness of the file has to be maintained throughout the process. When the private key is applied for both encryption and decryption through the cloud and when verifying the file is done by applying the mathematical procedure like linear program equations, makes the security more lenient and also achieves this through the efficient cost range and maintains the best outcome.
Vogel's Approximation method can be refined for all the nonlinear programming methods for optimizing the proper transportation cost. It produces the optimizing solution for transferring the files from one way to another. A better example for the Vogel's Approximation method is:

Server	Supply
A	120
B	80
C	80

Client	Demand
P	150
Q	70
R	60

	P	Q	R
A	8	5	6
B	15	10	12
C	3	9	10

To find the initial feasible solution for the above example using Vogel's approximation method, we must find the penalty cost for both the rows and columns of the problem.
Penalty cost = Lower Penalty cost – next Lower Penalty cost
Row A 6-5 =1
Row B 2-10=2
Row C 9-3 =6
Column P 8-3=5
Column Q 9-5=4
Column R 10-6=4
Compare the penalty cost of Rows and Column and we can find that 6 has the highest penalty cost.
We are using the dual simplex problem for the simple linear equation,
Minimize z = 2x1 + 3x2 + 4x3 + 5x4
subject to x1 −x2 +x3 −x4 ≥ 10,
x1 −2x2 +3x3 −4x4 ≥ 6,
3x1 −4x2 +5x3 −6x4 ≥ 15

x1, x2, x3, x4 ≥ 0. (1)

All coefficients in z = 2x1 + 3x2 + 4x3 + 5x4 are non-negative, therefore it is optimal for the dual simplex. Multiply the equations by −1 and add to each of the equations its own variable.

The Framework of the Algorithm

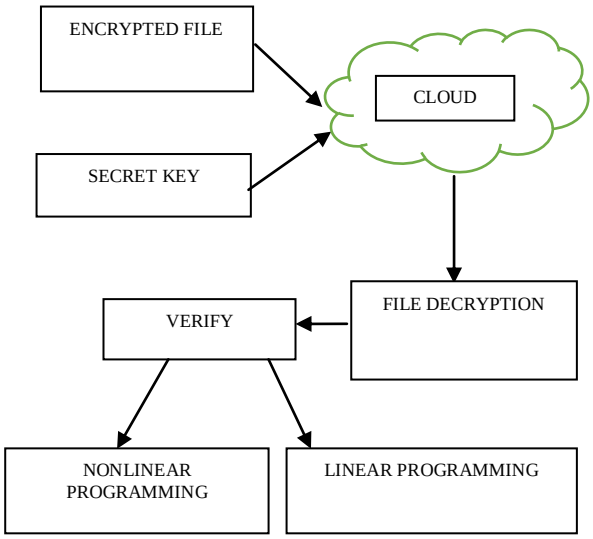
The Framework uses four Algorithms, where Proof Generation Algorithm is used by the Cloud Server and Client process uses three algorithms organized as Key Generation, Problem Encryption, Result Decryption respectively. The Algorithm can be detailed as below:[18\

- Key Generation Algorithm: This can be used for randomly generating the private key which produces a secret key 'K'. This 'K' is generated when encrypt process happens to the file and sent to the user through the cloud.
- Problem Encryption Algorithm: This encrypts the selected multiple files requested by the user along with generation of secret key 'K'. It encrypts the file and thus gets processed in the cloud.
- Proof Generation Algorithm: This algorithm is used mainly for outsourcing and thus provides a verification solution similar to the output produced. The verification solution maintains the efficiency of the output and it checks for the possibility of the errors.
- Result Decryption Algorithm: This decrypts the encrypted file sent via the cloud. Since the decryption process takes after the verification, it provides much accurate results and thus the original file content will be decrypted and proper results will be shown.

3. Related Works

In this section, we will review some existing methods which have been proposed in past years. Atallahet. al. [1][2] has been proposed the general computation methods for securely outsourcing of linear algebraic equations and also for real-time complex matrix multiplications. They have mentioned the sensitive information can be accessed. Peeter Laud et. al. [3] discussed about the practicality of outsourcing linear programming. Benjamin and Atallah [4] discussed the difficulty of secure outsourcing for broadly applicable linear algebra calculations. However, the proposed protocol demands the costly operations of homomorphic encryptions. In past recent years, Wang et. al. [5] introduced a secure outsourcing methodology for the large-scale system of the linear equations, which is based on the iterative approaches. However, it needs multi-round co-operations between the client and the cloud server and thus is quite impractical. Wang et al. [6] introduced effective mechanisms for secure outsourcing of linear programming computations. But the solution demands various matrix to matrix operations, which will possess cubic-time computational complexity, so is less feasible. The forms of mathematical linear computations that include matrix multiplications, comparisons of efficiency are hard for large problems. To avoid these complexities, either heavy cloud-side encryption and decryption can be performed [7][8] or large complexities [9][10] [19] are required.

4. System Model



5. Conclusion

This paper provides the optimal solution to the security of outsourcing done in the cloud and provides feasibility to both the linear and nonlinear programming functions. Secure computations are done through the cloud. The algorithms and methods are used for the security of the data owned by the user. It not only provides cryptographic security to the data but also the correctness of the data through the verification methods. Thus, improper data access can be restrained.

References

[1] Atallah M & Frikken K, "Securely outsourcing linear algebra computations", *Proc. 5th ACM Symp.Inf., Comput.Commun. Security*, (2010), pp.48-59.

[2] Atallah MJ, Pantazopoulos KN, Rice JR & Spafford EH, "Secure outsourcing of scientific computations", *Adv. Comput.*, Vol.54, (2002), pp.215-272.

[3] Laud P & Pankova A, "On the Impossibility of Privately Outsourcing Linear Programming", *ACM* CCSW, (2013).

[4] Benjamin D & Atallah MJ, "Private and cheating-free outsourcing of algebraic computations", *Proc. 6th Annu. Conf. Privacy, Secur. Trust (PST)*, (2008), pp.240-245.

[5] Wang C, Ren K, Wang J & Wang Q, "Harnessing the cloud for securely outsourcing large-scale systems of linear equations", *IEEE Trans. Parallel Distrib. Syst.*, Vol.24, No.6, (2013), pp.1172-1181.

[6] Wang C, Renand K & Wang J, "Secure and practical outsourcing of linear programming in cloud computing", *Proc. 30th IEEE Int. Conf. Comput.Commun. (INFOCOM)*, (2011), pp.820-828.

[7] Mell P & Grance T, "Draft nist working definition of cloud computing-v15", (2009), 123-135.
http://csrc.nist.gov/groups/SNS/cloud-computing/index.html.

[8] Hohenberger S & Lysyanskaya A, "How to securely outsource cryptographic computations", *Proc. of TCC*, (2005), pp.264-282.

[9] Gennaro R, Gentry C & Parno B, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers", *Proc. of CRYPTO*, (2010).

[10] Yu S, Wang C, Ren K & Lou W, "Achieving secure, scalable, and fine-grained access control in cloud computing", *Proc. of IEEE INFOCOM?*, (2010).

[11] Mangasarian OL, "Privacy-preserving linear programming", *Optimization Letters*, Vol.5, No.1,(2011), pp.165-172.

[12] Vaidya J, "Privacy-preserving Linear Programming", *Proc. 24th ACM Symp.Appl.Comput.*, (2009), pp.2002-2007.

[13] Wang C, Ren K & Wang J, "Secure optimization computation outsourcing in cloud computing: A case study of linear programming", *IEEE transactions on computers*, Vol.65, No.1, (2016), pp.216-229.

[14] Li J & Atallah MJ, "Secure and private collaborative linear programming", *Proc. Int. Conf. Collaborative Comput.*, (2006), pp.1-8.

[15] Optimization of Resource Provisioning cost in cloud computing, http://ieeexplore.ieee.org/iel5

[16] Cloud computing for optimization, http://www.mcs.anl.gov/files/ 2013/01.

[17] 3 ways of cloud optimization to improve efficiency of the cloud, http://www.datapipe.com/2015/01/29.

[18] A Akhmetbekova, P Auyesbayeva, Sh Ibrayev (2018). Turkic "Hikaya" genre and its characters. Opción, Año 33. 81-106.

[19] A Mukanbetkaliyev, S Amandykova, Y Zhambayev, Z Duskaziyeva, A Alimbetova (2018). The aspects of legal regulation on staffing of procuratorial authorities of the Russian Federation and the Republic of Kazakhstan Opción, Año 33. 187-216.