International Journal of
Science and Engineering Investigations vol. 6, issue 69, October 2017
ISSN: 2251-8843

Cloud Computing Security Solution Based on GRC Method and Fully Homomorphic Encryption Algorithm in a Private Cloud

H. R. Semsar[1], P. Daneshjoo[2], M. H. Rezvani[3]
[1,2]Department of Computer Engineering, West Tehran Branch, Islamic Azad University, Tehran, Iran
[3]Department of Electrical, Computer and IT Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran
([1]dr110hrs@gmail.com, [2]pdaneshjoo@gmail.com, [3]mhossein.rezvani@gmail.com)

***Abstract*-**This article, by presenting a security strategy for cloud computing used the GRC method, analyzes the different sections of this approach and classification to create security policies and frameworks; And due to the importance of the security and the speed with each other, it used symmetric, homomorphic encryption algorithms, with the MORE approach; The method introduced in this article examined information when sending from the source, during the exchange, calculation of big data and storage, with the speed and security in the private cloud.

Keywords- *Cloud Computing, Security, GRC Method, Fully Homomorphic Encryption Algorithm, MORE Approach, Secure Cloud, Private Cloud*

I. INTRODUCTION

Cloud computing is a computational paradigm, as well as a distributed architecture, with the main purpose of providing secure, fast, and convenient storage of network computing data and services, with all the computing resources provided as services and provided on the Internet, Cloud computing provides cost-effective tools that provide IT services and access to dynamic, scalable, and virtual environments [1].

Considered the importance of cloud computing for governments and large organizations and corporations, it is necessary to consider the disadvantages and problems of this technology; one of the major issues that are addressed in this paper is the security issue using a GRC method and a symmetric Fully Homomorphic encryption algorithm with the MORE approach examines different security layers.

To this end, in [1], the early definition of cloud computing and the introduction of the GRC method have been addressed; In [2], the introduction of security and standard infrastructure has been addressed; In [3] the risk management perspective in cloud computing investigated; In [4-8] introduced and accurately investigated the types of homomorphic encryption algorithms and some of its advantages and disadvantages ;In [9], the method of asymmetric homomorphic encryption algorithm has been investigated; And in [10], the MORE approach investigated.

II. INFORMATION SECURITY INFRASTRUCTURE

When building a building for a museum or a goldsmith, the design and construction of the very first stages should be thought of as security, otherwise locking is not profitable. Reinforced concrete walls to Steel, Secure flooring, defining and blocking all possible channels are pre requirement for a secure building [2].

Information security is not separate from this; if it is supposed to provide a service in a network, it must first determine the (specific) threats and (risk) and then, by specifying the security margin, the investment required for security measures is calculated and based on it an appropriate architecture to predict [2].

No matter how powerful the cryptography system is, But there is the possibility of infiltration to it; the most powerful way of encrypting the world in front of the user who writes his password in his notebook and lost his notebook somewhere is weak; therefore, the training of managers, Employees and users are also worthy the attention as much as using expensive systems (attack detection). Table I. provided a template for a secure architecture for information [2].

TABLE I. A MODEL OF SECURE ARCHITECTURE

Application-compatible security prediction	
Managing vulnerable spots Includes analysis, discovery, inspection and modification of security holes and periodic review and testing	**Manage Threats** Includes analysis, prevention, guarantee and identify ways out of the crisis and estimate the amount of damages possible
Network Infrastructures Security	
Technical security Includes providing security services at the hardware, software, operating system and network level	**Organizational Security** Including defining the security structure and the process of protecting information, personnel training and users and approval of the law and the rules for determining the violation

III. SECURITY MODEL FOR CLOUD

Figure 1 illustrates governance, risk management and compliance as effective in each layer of the security program; Security in the application layer is critical to the effective implementation of access policies; physical infrastructure security is very important because It provides more effective control over the infrastructure; the physical presence of the infrastructure in the organization is always an important element of identity. (Otherwise, physical access can seriously endanger security) Through the security model, you can find out more about this issue [1].

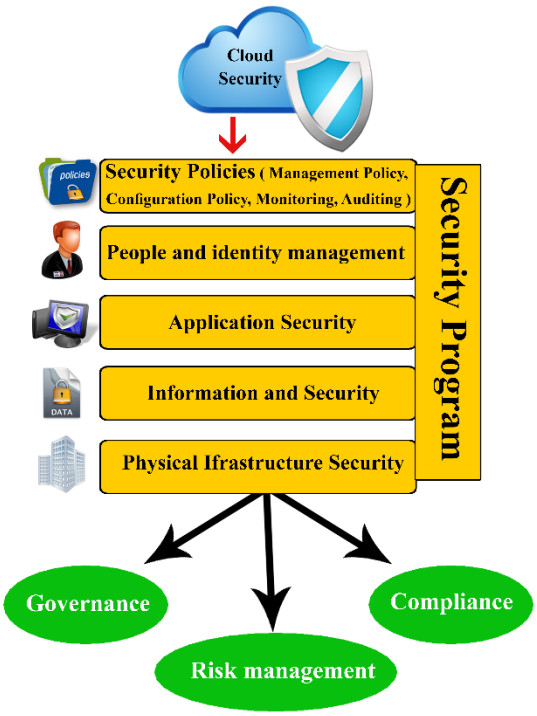

Figure 1. A security model for cloud computing

IV. SECURITY GRC METHOD

The basic responsibility of the organization is to identify, implement process, controls, and structure the organization that obtains effective GRC cloud security [1].

A. *Governance*

Any activity that leads to the regulation and creation of policies, rules and technologies that are directed at the organization to achieve the security goal. Some organizational responsibilities such as: cloud provider access risk, sensitive information protection, legal issues understanding, information lifecycle management, portability and interoperability, the organization must implement a framework for more effective risk management and risk management functionality using Measure out specific metrics [1].

B. *Risk Management*

Select a cloud provider and implement security and privacy controls, their effectiveness, efficiency, and their constraints based on applicable rules, guidelines, policies, standards or regulations that the provider must comply with; Cloud consumers have certain unknown requirements and missions and therefore a core set of designs should be designed [3].

Risk management is a collection of processes that manage threat identification, risk analysis and design of a countermeasure solution. In fact, risk management responds to threats internal and external in the organization

C. *Compliance*

In fact, after legislating and policy-making and designing responses to risks and threats, it is necessary to implement and enforce all stages beforehand; these rules can be a set of internal rules, frameworks and policies, or can be a set of The external standards are to Supervising and adhering to this, is part of the compliance policies.

D. *People and Identity Management*

Only the user is allowed to access the organization's assets; the Identity Federation or authentication and licensing approach should be applied; it should rely on the ability to register for the user who wants to enter. Identity management, provides Directory service leveraging for access control [1].

E. *App Security*

The cloud provider should follow a secure development process; Xml digital signature and XML encryption should be used to protect applications against XML attacks and web service attacks [1].

Monitoring method can be an appropriate security solution for prevention and security.

F. *Physical Infrastructure Security*

Protection or safeguards include biometric access control, CCTV surveillance, Doors should be alert, the use of a computer that has an access control system and restricts access with logos and labels; this system Allows access only by issuing a license [1].

G. *Information Security*

The highest concern at this stage is data and information security, the need to focus on how data is stored, adapted processing, auditing, standard encryption and encryption key management should lead to data privacy protection, security policy and the trusted virtual domain must be implemented so that the problem data or information is resolved. Intrusion detection and prevention system must be built [1].

V. HOMOMORPHIC ENCRYPTION METHOD

The Webster Dictionary of Homomorphism is defined as follows: a mapping of a mathematical set (such as a group, ring, or vector space) into or onto another set or itself in such a way that the result obtained by applying the operations to elements of the first set is mapped onto the result obtained by

applying the corresponding operations to their respective images in the second set [4].

Homomorphic encryption users Information security leave the computer from the moment data flows, until it returns, should be provide.

This method requires that all the mathematical and logical operations required in the calculations, which may be represented by circuits or gates, are applied to the data encryption form [5].

Homomorphic encryption can encrypt most of the shared information and delete decryption operations. Homomorphic was first proposed by Rivest and his colleagues in 1978; [6] and Craig Gentry in his Ph.D. Thesis in 2009 introduced the fully homomorphic encryption method [5].

Homomorphic encryption consists of three concepts, Partially Homomorphic Encryption (PHE), Some What Homomorphic Encryption (SWHE) and Fully Homomorphic Encryption (FHE).

The PHE enables us to perform an operation, such as multiplication or addition, but not both, on encrypted data, in SWHE, it can perform more than one operation, but only a limited number of addition And multiplication operations and operations can support, a cryptosystem that supports and supports both addition and multiplication operations and can calculate any function is known as a FHE system [5].

The value of using FHE is more than PHE and SWHE, because using this model, circuits can be evaluated in a coordinated manner, which in turn allows the creation of programs that may run on encrypted inputs Which leads to the successful production of the encrypted output because the inputs of these programs are never decrypted [5].

A. Principles of AFHE Method

In [7], an example of the main principles of the asymmetric fully homomorphic algorithm (AFHE) method is introduced; the homomorphic encryption method has not been applied asymmetrically because of some problems to date. Of course, method is asymmetric partially homomorphic algorithm (APHE) using algorithms (such as: RSA, ElGamal, Diffie-Hellman, Paillier, Goldwasser-Micali, Benaloh, Blum-Goldwasser), but these methods are not known as an FHE algorithm. The reason for this problem is the existence of computational noise and overhead in a large volume of data and the mismatch of math's in addition and multiplication operation; however, there are solutions to noise in [5] for the asymmetric method, and in [8] for the symmetric method, but asymmetric methods have been slow to carry out calculations has led to the lack of an efficient AFHE method, so far, this method requires further studies.

B. SFHE Method

All algorithms available for the homomorphic method are not efficient because of the computational complexity of the asymmetric approach, such as the Gentry and DGHV [9] methods, In [10], a symmetric fully homomorphic algorithm (SFHE) approach, such as matrix operation for randomization and encryption (MORE), is introduced with homomorphic properties.

This approach is based on matrix computations, which is as follows:

- Encryption algorithm: The encryption algorithm is as follows, in which m is the plaintext, , r is a random integer in a loop such as Z_N, K is a reverse matrix in Z_N (2×2) and K^{-1} is inverse of it:

$$E(m,k) = K^{-1}\begin{bmatrix} m & 0 \\ 0 & r \end{bmatrix} K \quad (1)$$

- Decryption algorithm: The Decryption process is simply a reverse encryption process that applies:

$$D(m,k) = KE(m,k)K^{-1} = \begin{bmatrix} m & 0 \\ 0 & r \end{bmatrix} \quad (2)$$

- Additive property verification:

$$E(m_1) + E(m_2) = K^{-1}\begin{bmatrix} m_1 & 0 \\ 0 & r_1 \end{bmatrix} K + K^{-1}\begin{bmatrix} m_2 & 0 \\ 0 & r_2 \end{bmatrix} K \quad (3)$$

$$= K^{-1}\begin{bmatrix} m_1 + m_2 & 0 \\ 0 & r_1 + r_2 \end{bmatrix} K = E(m_1 + m_2)$$

- Multiplicative property verification:

$$E(m_1) \times E(m_2) = K^{-1}\begin{bmatrix} m_1 & 0 \\ 0 & r_1 \end{bmatrix} K \times K^{-1}\begin{bmatrix} m_2 & 0 \\ 0 & r_2 \end{bmatrix} K \quad (4)$$

$$= K^{-1}\begin{bmatrix} m_1 \times m_2 & 0 \\ 0 & r_1 \times r_2 \end{bmatrix} K = E(m_1 \times m_2)$$

It can be seen that the MORE approach is FHE, because it fully satisfies both homomorphic properties [10].

C. Calculation of Algorithm Processing Speed in Cloud Computing

As mentioned in the previous section, due to the high speed of symmetric encryption methods, the MORE approach can also be proposed as an appropriate option for the information security sector in the GRC method, an example of how fast this algorithm performs in cloud computing with big data is according to Figure 2.

As in most simulations, loops are used to replicate and generate sequential random data; in this simulation, used the MATLAB software, the loops are optimally generated to produce random numbers, replicates and Evaluation has been used. The loop time in simulation is a significant amount of program code; the average run time in two modes of multiplication and addition of the MORE approach in 5 types of data inputs based of bytes, with 10,000 repetitions per entry, is visible in the figure.

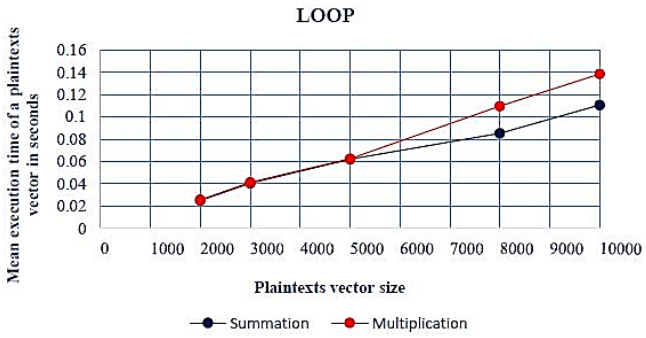

Figure 2. Mean time execution algorithm in Loop

In Figure 3 the time of calculation of the encryption algorithm has been investigated in multiplication and addition, and, as in the previous figure, in 5 inputs based of bytes, with 10,000 repeat times for each input are investigated.

The difference between some of the numbers was obtained in 0.0001 in difference. The numbers used in the figures are given in Table II.

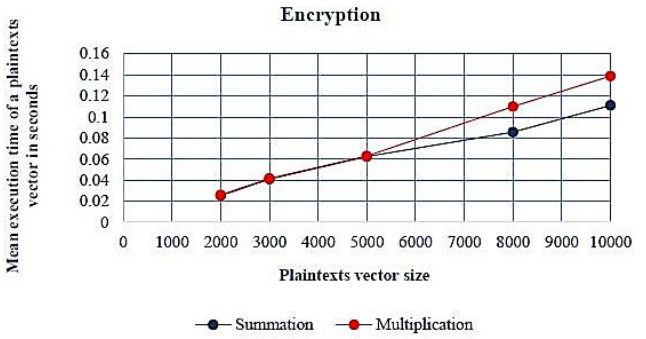

Figure 3. Mean time execution in encryption algorithm

In Figure 4, the decoding algorithm is investigated, which is the last step in simulation of the algorithm, at this point, the encrypted data is decrypted in accordance with previous inputs and ciphertext obtained in the previous step. As expected, the average execution time of the encryption algorithm with the average execution time of the decryption algorithm has a very small difference, which this case is symmetric encryption properties.

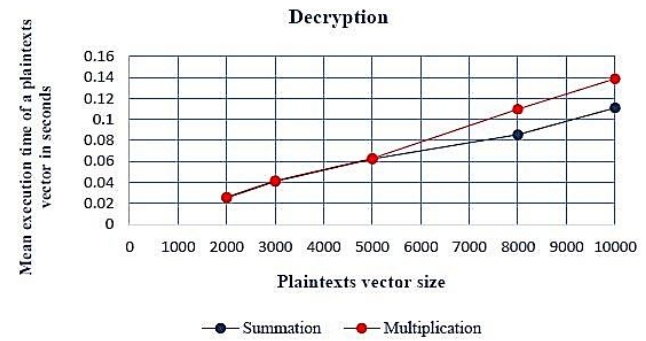

Figure 4. Mean time execution in decryption algorithm

The difference in the numbers obtained from 3 simulations, loops, encryption and decryption is given in table 2.

TABLE II. THE NUMBERS OBTAINED FROM THE SIMULATION

Summation			
Byte	LOOP	ENC	DEC
2000	0.0252	0.0252	0.0253
3000	0.0408	0.0409	0.0409
5000	0.0623	0.0624	0.0624
8000	0.0855	0.0856	0.0856
10000	0.1108	0.1108	0.1109

Multiplication			
Byte	LOOP	ENC	DEC
2000	0.0258	0.0259	0.0259
3000	0.0415	0.0416	0.0416
5000	0.0626	0.0627	0.0627
8000	0.1097	0.1097	0.1098
10000	0.1386	0.1387	0.1387

The data in Table II, implementation of the MORE encryption algorithm using the MATLAB software on the Asus laptop with specifications:

Intel Core i7-5500U CPU @ 2.4GHz up to 3 GHz, 2 Core (s), 4 Logical Processor (s), 8GB RAM DDR3L up to 12GB VRAM is done in parallel processing.

VI. CONCLUSION

This article examines the various sections of the strategic, standard and dynamic method called GRC for cloud computing security and in information security layer in the GRC method, to perform calculations, Exchange and store information with Appropriate pace, In clouds with a large amount of data encountered, And need to be provided secured dynamically; From completely homomorphic encryption algorithm has been used symmetrically with the MORE approach.

This method, while maintaining the security of the private cloud, is cost effective and very fast, scans the data, and performs computations on the data. This article, is the first fully article to present a security solution used the GRC method and the fully homomorphic encryption algorithm symmetrically in a private cloud.

REFERENCES

[1] F. S. Al-Anzi, S. Kr. Yadav and J. Soni, "Cloud computing: Security model comprising governance, risk management and compliance," IEEE International Conference on Data Mining and Intelligent Computing (ICDMIC), India, New Delhi, November 2014. doi: 10.1109/ICDMIC.2014.6954232

[2] A. Malekian and A. Zakeralhosseini, Data security, 6rd ed., Tehran: Nass, 2015, pp. 20-21.

[3] M. Iorga and A. Karmel, "Managing Risk in a Cloud Ecosystem," IEEE Cloud Computing Journal, vol. 2, pp. 51-57, Nov-Dec 2015. doi: 10.1109/MCC.2015.122

[4] Merriam-Webster dictionary, (https://www.merriam-webster.com/dictionary/homomorphism).

[5] M. Ogburn, C. Turner and P. Dahal, "Homomorphic Encryption," Elsevier on Procedia Computer Science, vol.20, pp. 502-509, November 2013. https://doi.org/10.1016/j.procs.2013.09.310

[6] Q. Meng and Ch. Gong, "Research of cloud computing security in digital library," 6th International Conference on Information Management, Innovation Management and Industrial Engineering (ICIII), November 2013. doi: 10.1109/ICIII.2013.6703173

[7] F. Zhao, Ch. Li, Ch. F. Liu, "A cloud computing security solution based on fully homomorphic encryption," IEEE 16th International Conference on Advanced Communication Technology, South Korea, Pyeongchang, March 2014. doi: 10.1109/ICACT.2014.6779008.

[8] J. Li and L.Wang, "Noise-free Symmetric Fully Homomorphic Encryption based on noncommutative rings," International Association for Cryptologic Research (IACR) Cryptology ePrint Archive, Oct 2015. http://ia.cr/2015/641

[9] M. Van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan, "Fully Homomorphic Encryption over the Integers," Springer: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, vol. 6110, pp. 24-43. 2010. https://link.springer.com/chapter/10.1007/978-3-642-13190-5_2

[10] K. Hariss, H. Noura and A. E. Samhat, "Fully Enhanced Homomorphic Encryption algorithm of MORE approach for real world applications," Elsevier on Journal of Information Security and Applications, vol. 34, pp. 233-242. June 2017.

Hamid Reza Semsar was born in Tehran, Iran, in Oct 1989. He received the B.S. degree in Information Technology Engineering from the Iran University of Science & Technology (IUST), Tehran, Iran in 2014. He is currently MSc. Student in Information Technology Engineering from the West Tehran Branch, Islamic Azad University (WTIAU), Tehran, Iran. Since 2013 he has researched about cloud computing and secure cloud and published several papers related to this field. Eng. Semsar's research interests include cloud computing, Security, fog computing, virtualization.

Parisa Daneshjoo was born in Tehran, She received her B.Sc. degree in Computer Software Engineering in 1996, from Islamic Azad University, South Tehran Branch, and Tehran, Iran. She received her M.Sc. degrees in Computer Software Engineering in 2008 from Tarbiat Modares University, Tehran, Iran and received Ph.D. degrees in Software Engineering in 2015 from Islamic Azad University, Science and Research Branch, Tehran, Iran. Respectively. She held the position of Assistant Professor in Islamic azad university west Tehran branch (WTIAU). She was Head of Department, Computer engineering in Islamic azad university west Tehran branch, Tehran, Iran (WTIAU) in 2015-2017.

Mohammad Hossein Rezvani was born in Tehran, in 1975. He received his B.Sc. degree in Computer Hardware; Computer Engineering from Amirkabir University of Technology - Tehran Polytechnic, Tehran, Iran . He received his M.Sc. and Ph.D. degrees in Computer Systems Architecture; Computer Engineering in 1999 and 2005 from Iran University of Science and Technology (IUST), Tehran, Iran, respectively. He held the position of Assistant Professor in Qazvin Islamic Azad University (QIAU).