International Journal of
Science and Engineering Investigations vol. 6, issue 70, November 2017
ISSN: 2251-8843

Improvement GRC Security Solution Using SFHE-PORE Algorithm in Cloud Computing

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*-**One of the most important subjects in technologies, According to the researchers of computer science and information technology is cloud computing, it has more benefits that included: Facilitating resource management, better availability, Reducing costs, In addition to, there are more problems that one of these is Maintaining security dynamically; To create dynamic security, this requires for a comprehensive plan; In this paper introduced and survived of Strategic approach of GRC; Planning and providing a safe and fast solution are associated parts of this method for data exchanging and data making storage; Therefore, We introduced the best methods for encryption calculations by presenting and examining a symmetric fully homomorphic encryption algorithm; finally, The best method is presented by a comparative evaluation of performing of these methods, The proposed method has a good speed in clouds with high traffic.

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

I. INTRODUCTION

Considered the importance and applicability of cloud computing in various fields, the attention of most researchers has attracted to this technology; But security is a major dilemma, that this technology faces; this article addresses the issue of security by using the improve GRC security method and the symmetric fully homomorphic encryption method; Using different experiments, it introduces the most optimal approach in symmetric fully homomorphic encryption.

For this purpose, in [1], the early definition of cloud computing and the introduction and review of the GRC method have been addressed; In [2], the introduction of security and standard infrastructure have been addressed; In [3] explored the risk management perspective in cloud computing; In [4-8] introduce examined the types of homomorphic encryption algorithms and some of its advantages and disadvantages; In [9], the method of asymmetric homomorphic encryption algorithms have been investigated; In [10], Matrix Operation for Randomization and Encryption (MORE) approach was explored and In [11] the MORE approach, Polynomial Operation for Randomization and Encryption (PORE) approach, and A solution to implement these two approaches have been addressed.

II. CLOUD COMPUTING AND SECURITY ISSUES

Cloud computing is an emerging technology that brings online IT services, demand-side sharing and cost-cutting.

The cloud has many benefits, but in security issues still suffer from this weakness. One of the outstanding security issues that is raised is the compliance and privacy that is discussed in Table I. in this regard [1].

TABLE I. SECURITY THREATS IN CLOUD ENVIRONMENTS

Threat(According to Cloud security Alliance(CSA))	Description
Abuse and Nefarious Use of Cloud Computing	This is the worst threat to cloud computing, such as botnets
Insecure API	Cloud security depends on the security of the interface, APIs should be implemented at the secure access level, using authentication methods and encryption mechanisms.
Malicious Insiders	Malicious intruders can access unauthorized access to cloud resources
Customer-data manipulation	Sql injection and command injection, insecure direct object references, cross-site scripting are among these attacks.
Data Loss/Leakage	Data leakage occurs when the data falls into the wrong person's hands and it starts to stored, transferred, and processed data.
Account, Service & Traffic Hijacking	The same is stealing accounts Such as: man-in-the middle attacks, phishing, and denial of service attacks
Data scavenging	The data is not completely eliminated and the attacker can reconstruct the data.
Malicious VM creation	An attacker can create a VM image which consist of malicious code such as a Trojan horse and store it in the provider repository.

III. ESSENTIAL STEPS FOR CLOUD SECURITY

The essential steps for cloud security are shown in Figure 1, which is presented in the form of six essential steps. These steps are: 1) Asset classifications / Identify asset for cloud development. 2) Evaluate sensitivity of asset. 3) Map asset to appropriate security model. 4) Evaluate the security provided by service provider. 5) Map the data flow between provider and organization. 6) Understand how under will access the data and information in organization [1].

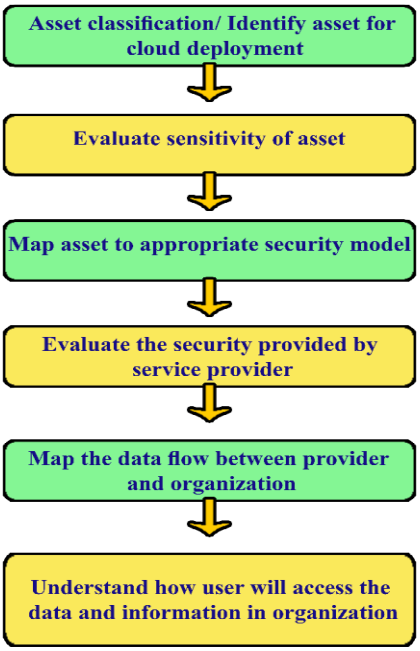

Figure 1. Essential steps for cloud security

IV. 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].

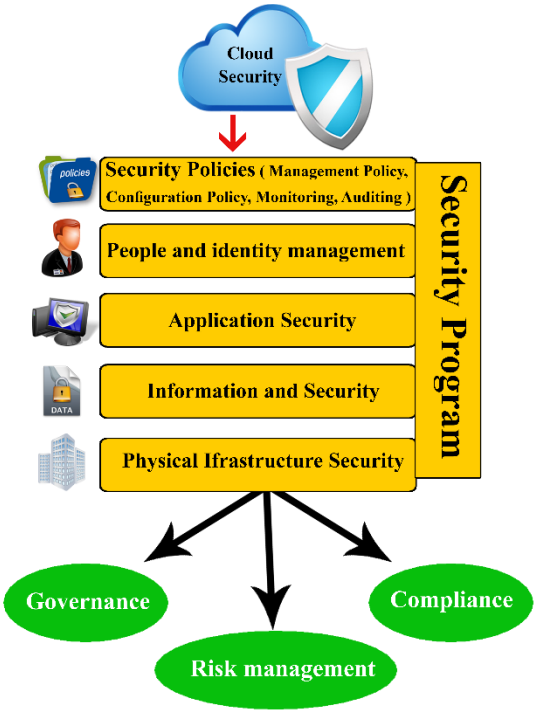

Figure 2. A security model for cloud computing

V. 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].

VI. 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 due to the computational complexity of the asymmetric technique, such as Gentry and DGHV [9] method and In the following, two symmetric approaches, called MORE and PORE, with homomorphic properties are introduced [10].

- The MORE approach, based on matrix computing, is an operation that is in accordance with Table II:

TABLE II. MORE APPROACH

Stages	Equations
In this approach, 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.	
Encryption Algorithm	$E(m,k) = K^{-1}\begin{bmatrix} m & 0 \\ 0 & r \end{bmatrix} K$
Decryption Algorithm	$D(m,k) = KE(m,k)K^{-1} = \begin{bmatrix} m & 0 \\ 0 & r \end{bmatrix}$
Additive property verification	$E(m_1) + E(m_2) = K^{-1}\begin{bmatrix} m_1 & 0 \\ 0 & r_1 \end{bmatrix} + K^{-1}\begin{bmatrix} m_2 & 0 \\ 0 & r_2 \end{bmatrix} K$ $= K^{-1}\begin{bmatrix} m_1 + m_2 & 0 \\ 0 & r_1 + r_2 \end{bmatrix} K = E(m_1 + m_2)$
Multiplicative property verification	$E(m_1) \times E(m_2)$ $= K^{-1}\begin{bmatrix} m_1 & 0 \\ 0 & r_1 \end{bmatrix} \times K^{-1}\begin{bmatrix} m_2 & 0 \\ 0 & r_2 \end{bmatrix} K = K^{-1}$ $= K^{-1}\begin{bmatrix} m_1 \times m_2 & 0 \\ 0 & r_1 \times r_2 \end{bmatrix} K = E(m_1 \times m_2)$

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

This approach is based on polynomial calculations, which is as follows:

- To select the keys, two large random numbers in terms of mod N are considered to be v_1 and v_2, The polynomial calculations in the source are as follows [11]:

$$PP(v) = (v - v_1).(v - v_2) \bmod N = v^2 - bv + c \quad (1)$$

That:

$$b = -(v_1 + v_2) \bmod N \quad (2)$$

And:

$$c = (v_1 v_2) \bmod N \quad (3)$$

- Encryption algorithm: An encryption algorithm in which X_i is plaintext, R_i is a random integer in a loop such as Z_N, X_i ciphertext contains: (a_i, d_i) as follows:

$$X_i = a_i v_1 + d_i \quad (4)$$

$$R_i = a_i v_2 + d_i \quad (5)$$

The calculation of the two parameters (a) and (d) is as follows:

$$a_i = {}^{X_i - R_i}/_{v_1 - v_2} \quad (6)$$

$$d_i = X_i - a_i v_1 = {}^{R_i v_1 - X_i v_2}/_{v_1 - v_2} \quad (7)$$

- Decryption algorithm: If a_i and d_i are available and put in Equations 4 and 5, Encrypted text is decrypt.
- Additive property verification:

$$PORE(X_1) + PORE(X_2) = (a_1 + a_2, d_1 + d_2) \quad (8)$$

- Multiplicative property verification:

$$PORE(X_1) \times PORE(X_2) = \quad (9)$$

$$((a_1 + d_1).(a_2 + d_2) - a_1.a_2.(1 + b) - d_1 d_2,\ (d_1 d_2 - a_1.a_2.C)).$$

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

C. *Calculation of Algorithm Processing Speed in Cloud Computing*

As noted in the previous section, because of the high speed of symmetric encryption methods, two MORE and PORE methods for information security in the GRC method have been considered; a sample of the speed of the performance of these algorithms in cloud computing and big data in same conditions , As shown in Figures 3 and 4.

As in most simulations, loops are used to replicate and generate sequential random data; in this simulation, using the MATLAB software, the loops are optimally generated to produce random numbers, replicates 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 is in 5 types of data inputs based of byte, with 10,000 times the repeat for each input, checking Has been, which is visible in Fig. 3.

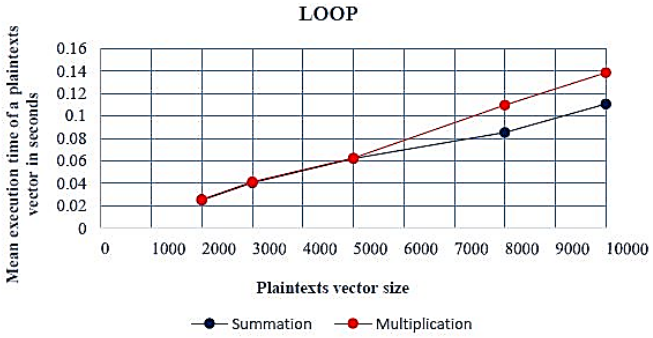

Figure 3. Mean time to execution loop in MORE approach

Figure 4 shows the speed of performance of the PORE approach in two modes of addition and multiplication with 5 types of data inputs based of byte, with 10,000 times the repeat for each input.

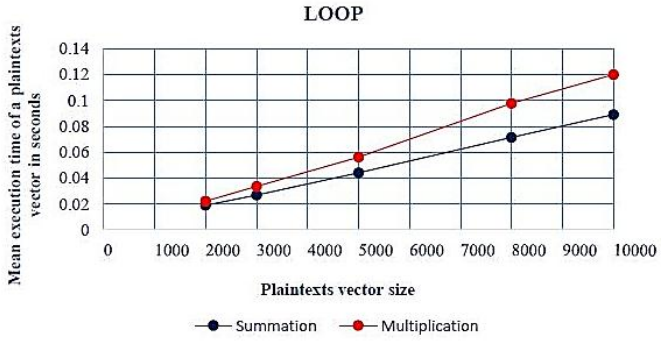

Figure 4. Mean time to execution loop in PORE approach

In Figure 3, the time of calculation of the encryption algorithm has been investigated in multiplication and addition in MORE approach, and, as in the figures 3 and 4 depicted, 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 Tables III and IV.

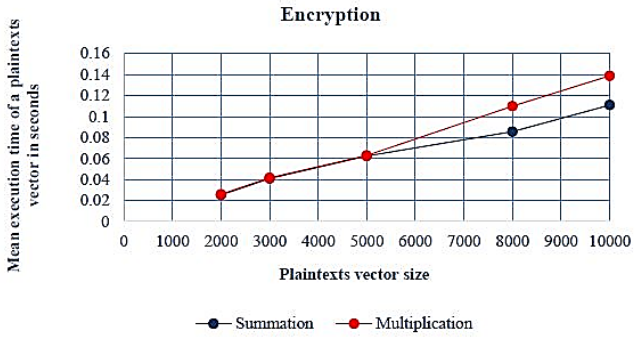

Figure 5. Mean time to execution encryption algorithm in MORE approach

Figure 6 examined the calculation time of the encryption algorithm in two modes multiplication and addition in the PORE approach, It can be seen that the volume of inputs increases; the average execution time of the algorithm increased in both the addition and the multiplication, but not equally.

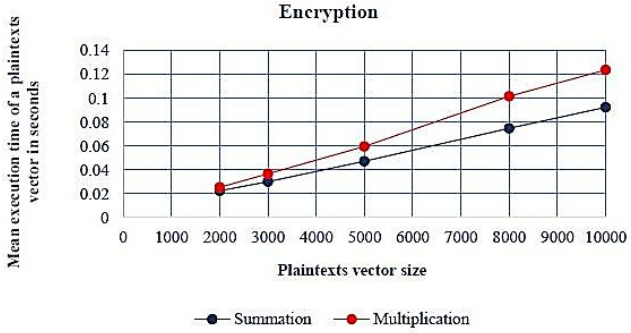

Figure 6. Mean time to execution encryption algorithm in PORE approach

In Figure 7, the decoding algorithm is investigated, which is the last step in simulation of the algorithm, at this point from the MORE approach, 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.

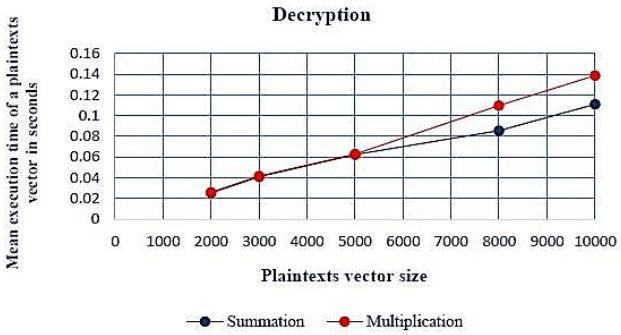

Fig. 1. Mean time to execution decryption algorithm in MORE approach

Figure 8 shown the average execution time of the decoding algorithm in the PORE approach;

It can be seen that the execution time of the decryption algorithm is roughly the same as the execution time of the encryption algorithm.

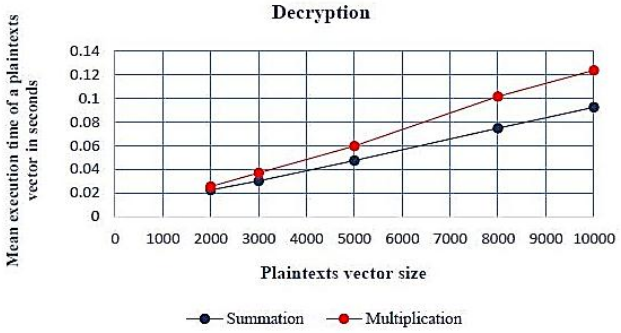

Figure 7. Mean time to execution decryption algorithm in PORE approach

In MORE approach, the difference in the numbers obtained from 3 simulations, loops, encryption and decryption is given in table III.

TABLE III. SIMULATION RESULTS IN THE MORE APPROACH

Summation					Multiplication			
Byte	LOOP	ENC	DEC		Byte	LOOP	ENC	DEC
2000	0.0252	0.0252	0.0253		2000	0.0258	0.0259	0.0259
3000	0.0408	0.0409	0.0409		3000	0.0415	0.0416	0.0416
5000	0.0623	0.0624	0.0624		5000	0.0626	0.0627	0.0627
8000	0.0855	0.0856	0.0856		8000	0.1097	0.1097	0.1098
10000	0.1108	0.1108	0.1109		10000	0.1386	0.1387	0.1387

In PORE approach, the difference in the numbers obtained from 3 simulations, loops, encryption and decryption is given in table IV.

TABLE IV. SIMULATION RESULTS IN THE PORE APPROACH

Summation					Multiplication			
Byte	LOOP	ENC	DEC		Byte	LOOP	ENC	DEC
2000	0.019	0.0225	0.0225		2000	0.0222	0.0254	0.0254
3000	0.0269	0.0302	0.0302		3000	0.0336	0.0368	0.0369
5000	0.0441	0.0473	0.0473		5000	0.0562	0.0596	0.0596
8000	0.0716	0.0748	0.0748		8000	0.0978	0.1016	0.1016
10000	0.0892	0.0925	0.0925		10000	0.1201	0.1238	0.1238

Tables III. And IV. Data, implementation of two MORE and PORE encryption algorithms using MATLAB software on 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.

Based on the comparison of the results of the simulations of the two approaches MORE and PORE, the performance of the SFHE algorithm with the PORE approach is much faster and improved than the MORE approach; Therefore, in the GRC scheme in the information security layer, the SFHE encryption algorithm with the PORE approach can be used as an improved solution.

VII. CONCLUSION

This paper examined security solution in the strategic plan and dynamic of GRC and its various layers to ensure security in cloud computing; Given the fact that in cloud computing, security and speed, the two concepts are completely interconnected, and speed plays an important role alongside security; So the need to use a method that ensure security and speed together.

For this purpose, in the information security layer of the GRC method, was introduced a fully homomorphic encryption algorithm symmetrically; And two different approaches to this algorithm, called the MORE and PORE approaches, have been investigated; According to the results of the simulation of the performance of these two approaches, The PORE approach had the complexity of encryption to maintain security, And faster processing speed than the MORE approach; Which proves the cost-effectiveness of this approach. And as a suggested solution in this paper for the information security layer in GRC has been proposed.

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.

[11] A. Kipnis and E. Hibshoosh, "Efficient Methods for Practical Fully-Homomorphic Symmetric-key Encryption, Randomization, and Verification," International Association for Cryptologic Research (IACR) Cryptology ePrint Archive, Nov 2012. http://ia.cr/2012/637

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).