Journal of Theoretical and Applied Information Technology
31st October 2015. Vol.80. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# ENHANCED DATA SECURITY APPROACH FOR CLOUD ENVIRONMENT BASED ON VARIOUS ENCRYPTION TECHNIQUES

**IBTIHAL MOUHIB, EL OUADGHIRI DRISS**

University Moulay Smail, Meknes, Morocco,

E-mail: imouhib2014@gmail.com, dmelouad@gmail.com

## ABSTRACT

Cloud Computing is the future of the next generation architecture of IT solutions , a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. Like any other technology cloud computing offer many advantages, however it still has some problems. One of the most challenging problems in Cloud Computing is the fact that the security and confidentiality of a remote resource cannot be technically validated by the customers, who can use the traditional methods of encryption (DES,AES,RSA…) to enhance the security of their data in the cloud .but they can't do any processing (searching, indexing…) on their data without giving their private keys to the cloud company .So there is a need for a mechanism to operate on encrypted data. A great interest has been growing homomorphic encryption a solution for discussed problem. In this paper we present first the cloud computing technology, then the security issues related to this technology, we will also explain the different methods of encryption and its applications to the cloud computing . Finally we propose our approach to evaluate and analyze the performance of the Traditional and Homomorphic encryption cryptosystems in cloud computing using OpenStack cloud environment .

**Keywords:** *Cloud Computing ,Security Issues,Data Security,Symmetric Encryption, Asymmetric Encryption, Homomorphic Encryption.*

## 1. INTRODUCTION

The Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or cloud provider interaction [1]. The current clouds are deployed in one of four deployment models:

- Private cloud : The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- Community cloud : The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g.,mission, security requirements, policy, and compliance considerations).
- Public cloud : The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- Hybrid cloud : The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Cloud computing architecture consists of three layers :SAAS,PAAS and IAAS. The Cisco view of cloud computing is all encompassing [2] , in terms of the architectural stack in a typical service value chain. These are services that are offered in a traditional IT data center. In a cloud value chain , they are virtualized and delivered on demand.

The three major layers in the cloud computing value chain are as follows:

- Software as a Service (SaaS) : is where application services are delivered over the network on a subscription and on-demand basis. Cisco WebEx™, Salesforce, Microsoft, and Google are a few providers in this layer.

- Platform as a Service (PaaS) : consists of run-time environments and software development frameworks and components delivered over the network on a pay-as-you-go basis. PaaS offerings are typically presented as Application Programming Interface (API) to consumers. Examples of this are: Google Apps Engine, Amazon Web Services, force.com, and Cisco® WebEx Connect.

- Infrastructure as a Service (IaaS) : is where compute, network, and storage are delivered over the network on a pay-as-you-go basis. Amazon pioneered this with AWS (Amazon Web Service), and now IBM and HP are entrants here also. The approach that Cisco is taking is to enable service providers to move into this area.

Cloud is a technology that everyone would love to take full advantage [3], it offers so much :

- Limitless Flexibility : With access to millions of different databases, and the ability to combine them into customized services.

- Better Reliability and Security : users no longer need to worry about their hardware failure, or hardware being stolen.

- Enhanced Collaboration : By enabling online sharing of information and applications, the cloud offers users new ways of working together.

- Portability : Users can access their data from anywhere.

- Simpler devices : With data stored and processed in the cloud, users simply need an interface to access and use this data, play games, etc.

- Unlimited Storage

- Access to lightning quick processing power.

## 2. SECURITY ISSUES IN CLOUD COMPUTING

Despite of all the advantages of the cloud there are significant security concerns that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments. The Cloud Security Alliance has identified the following threats as top security threats for cloud computing in 2013 [4]:

- Data Breaches : In a data breach, an actor is intentionally accessing data for malicious reasons. The challenge is that the measures put in place to mitigate one of the threats can exacerbate another. You could encrypt your data to reduce the impact of a breach, but if you lose your encryption key, you'll lose your data.

- Data Loss : data loss can be caused by employees who have no intention of causing a security incident , a loss can considerably introduce financial implications, legal ramifications, influence on trust between different actors related to a business and damage to reputation. Data Loss can occur due to malicious intent, accidental deletion by provider, or worse, a physical catastrophe leading to permanent loss.

- Account/Service and Traffic Hijacking : It is one of the major security threats to the cloud which leads to compromises on confidentiality, integrity and availability of deployed cloud services.

- Insecure APIs : The security of general cloud services is dependent upon the security of these basic APIs Cloud Providers expose a set of API for interacting customers to manage their data and interact with 3rd party applications for integrations.

- Denial of Service : DoS has always been an Internet threat, but it resurging in frequency and sophistication in the cloud. It can effect on cloud performance in general and can cause financial Losses [5] and can cause harmful effect in other servers in same cloud infrastructure as in [6].

- Malicious Insiders : malicious insiders could render security controls useless. He can steal confidential data of the cloud user, so the user is mostly left with trusting the cloud provider. [7] .A malicious insider can be an administrator who can easily inspect the virtual machines of cloud users and retrieve sensitive information

- Abuse of Cloud Computing : an example might be a malicious hacker using cloud servers to break an encryption key too

- Difficult to crack on a single computer, launch a DDoS attack, propagate malware, or share pirated software. The challenge here is for cloud providers to define what constitutes abuse and to determine the best processes to identify it.

- Insufficient Due Diligence : this threat giving rise to operational and architectural issues, or contractual issues over liability and transparency .

- Shared Technology Vulnerabilities : It can be duplicated across an environment where many virtual servers share the same configuration so understanding patch management and configuration management from the vendor becomes crucial.

By exploiting vulnerabilities in Cloud, an adversary can launch many attacks [8] such as :

- Cloud malware injection attacks : This type of attack , an adversary attempts to inject malicious service or code, which appears as one of the valid instance. If the attacker is successful, the cloud system automatically redirects valid user requests to the malicious service implementation, and the adversary's code is executed.

- Side channel Attacks : Traditional attacks on cryptographic algorithms use only the input and output of the algorithm, treating it like a monolithic black box. However,. Algorithms must be implemented in software and run on hardware, which have various properties (a physical quantity such as time, power consumption, electromagnetic radiation or sound ..) that change as a result of the cryptographic algorithm's execution. Side-channel attacks try to extract secret information based on some side-channel.

- Authentications attacks : Authentication is a weak point in hosted and virtual services and is frequently targeted. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers.

- Man in the middle Cryptographic Attacks : This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications.

- Denial of service attacks : that we have already explained in the last part.

## 3. TRADITIONAL ENCRYPTION TECHNIQUES

In our paper ,we are more interested in data Issues in Cloud Computing .It is a major issues with regard to security in a cloud based system. When data is on a cloud, anyone from anywhere anytime can access data from the cloud since data may be common, private and sensitive data in a cloud. So at the same time, many cloud computing service ,consumer and provider accesses and modify data. Thus there is a need of some data integrity method in cloud computing. For saving this data and making it still useful to the user, security must follow tenets named as the CIA Triad [9], which are confidentiality, integrity, and availability.

- Confidentiality : is to guarantee to customers that the other parties can not have access to their data.
- Integrity : means that no one has access to modify the data.

- Availability : is how many times the original user has access to the data.

To ensure the cloud computing data security , we usually use Encryption methods as a central technology .All cryptographic techniques in use today can be broadly classified as Symmetric and Asymmetric encryption .

Symmetric and asymmetric encryption schemes consists of the following algorithms :

| Algorithm | Symmetric encryption scheme | Asymmetric encryption scheme |
|---|---|---|
| KeyGen (λ) | Generates the secret key | Generates pairs of Public and Private Keys |
| Encrypt | Used for encryption of plain text to cipher text | Used for encryption of plain text to cipher text |
| Decrypt | Used for decryption of cipher text to plain text | Used for decryption of cipher text to plain text |

Table 1 : Algorithms of symmetric and asymmetric encryption schemes

### 3.1. Symmetric Cryptographic Techniques

In Symmetric cryptographic techniques , both sender and receiver share the same key which is used to both encrypt and decrypt messages. Sender and receiver only have to specify the shared key in the beginning and then they can begin to encrypt and decrypt messages between them using that key. Symmetric-key encryption can use either of the stream cipher or block cipher, where a stream cipher encrypts the bytes of a message one at a time and the block cipher take a number of bits as input and encrypt them as a single unit. This type of encryption is easy to carry out. All users have to do is specify and share the secret key and then begin to encrypt and decrypt messages. And it is much faster than asymmetric key encryption.The popular symmetric cryptographic algorithms are : DES, 3DES ,AES, Blowfish, RC5..

### 3.2. Asymmetric Cryptographic Techniques

In Asymmetric key cryptography, we use of two keys: a public key and a private key. The public key is made publicly available and is used to encrypt messages by anyone who wishes to send a message to the person that the key belongs to. The private key is kept secret and is used to decrypt received messages. It solves the problem of distributing the key for encryption. Everyone publishes their public keys and private keys are kept secret. However, the loss of a private key means that all received messages cannot be decrypted. Some of examples for asymmetric key cryptosystem are RSA, ELGAMAL, and ECC etc.

## 4. HOMOMORPHIC ENCRYPTION TECHNIQUES

### 4.1. Principe

The idea of homomorphic encryption was first proposed in 1978 by Rivest, Adleman and Dertouzos in their paper -On Data Banks and Privacy Homeomorphisms [10]. Homomorphic encryption use mechanisms similar to conventional cryptography, where plain texts and cipher texts both are treated with an equivalent algebraic function. Now the plain text and cipher text might also be not related but the emphasis is on the algebraic operation that works on both of them.

Homomorphic encryption scheme consists of the following four algorithms [ref] :

KeyGen (λ) : Input-the security parameter λ . Output-a tuple (Sk ,Pk) consisting of the secret key Sk and public key Pk.

Encrypt ( Pk,Pi ) : Input-a public key Pk and a plaintext Pi Output-ciphertext Ci

Decrypt (Sk ,Ci ) : Input-a secret key Sk and a ciphertext Ci .Output-the corresponding plaintext Pi

Evaluate(Pk C,Ci, ): Input-a public key Pk a circuit C with t inputs (of the set C of allowed circuits) and a set Pi of t ciphertext , Pi1 , Pi2, Pi3 , . . . .,Pit Output-a ciphertext Pi

### 4.1. Categories of homomorphic encryption

There are two types of homomorphic encryption schemes :

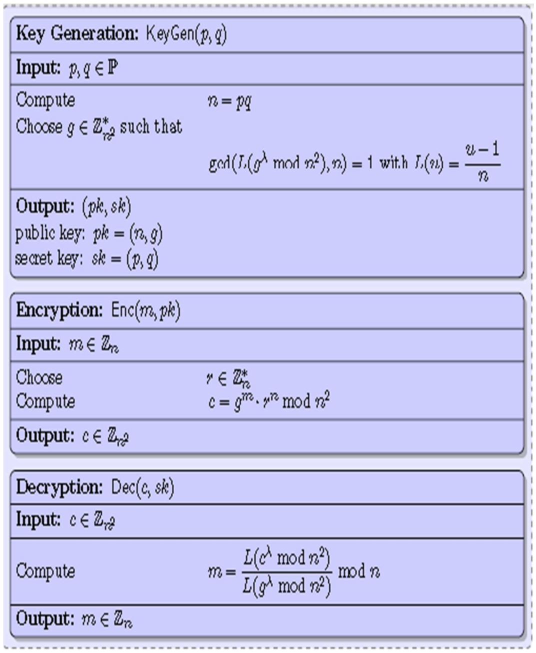
#### 4.1.1. Partially homomorphic encryption schemes

That includes schemes was able to support additions or multiplication computations :

#### *4.1.1.1. Additive Homomorphic Encryption schemes*

If an encryption algorithm is said to be additive homomorphic, then it support additive operations on encrypted data without the decryption of individual data's : $\mathrm{Enc}(x \otimes y) = \mathrm{Enc}(x) + \mathrm{Enc}(y)$

Example: Paillier Cryptosystem (1999): Paillier scheme [23] was proposed in 1999 based on arithmetic in the ring of integers modulo where is the product of two large primes.



**Key Generation:** KeyGen$(p, q)$
**Input:** $p, q \in \mathbb{P}$
Compute $n = pq$
Choose $g \in \mathbb{Z}^*_{n^2}$ such that
$\gcd(L(g^\lambda \bmod n^2), n) = 1$ with $L(u) = \frac{u-1}{n}$
**Output:** $(pk, sk)$
public key: $pk = (n, g)$
secret key: $sk = (p, q)$

**Encryption:** Enc$(m, pk)$
**Input:** $m \in \mathbb{Z}_n$
Choose $r \in \mathbb{Z}^*_n$
Compute $c = g^m \cdot r^n \bmod n^2$
**Output:** $c \in \mathbb{Z}_{n^2}$

**Decryption:** Dec$(c, sk)$
**Input:** $c \in \mathbb{Z}_{n^2}$
Compute $m = \frac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n$
**Output:** $m \in \mathbb{Z}_n$

*Figure 1 : Paillier cryptosystem*

In the Paillier cryptosystem, if the public key is the modulus m and the base g, then the encryption of a message x is $\mathcal{E}(x) = g^x r^m \bmod m^2$, for some random $r \in \{0, \ldots, m-1\}$.

The homomorphic property is then :

$$\mathcal{E}(x_1)\cdot\mathcal{E}(x_2) = (g^{x_1}r_1^m)(g^{x_2}r_2^m) = g^{x_1+x_2}(r_1r_2)^m = \mathcal{E}(x_1 + x_2 \bmod m)$$

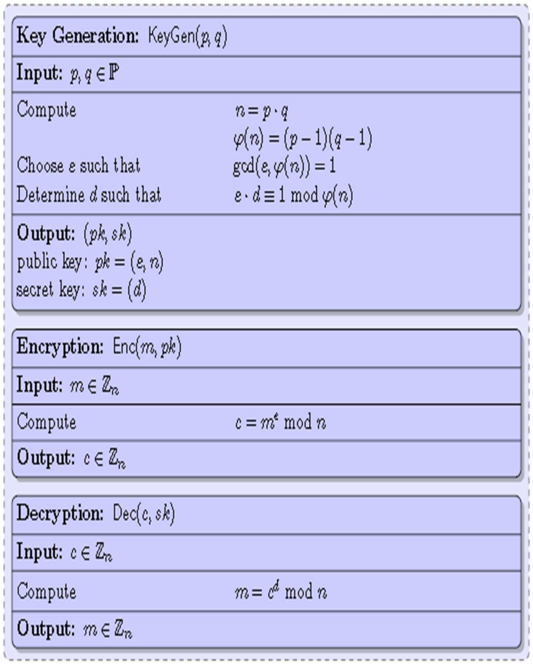
So, Paillier cryptosystem realizes the property of additive Homomorphic encryption. An application of an additive Homomorphic encryption is electronic voting: Each vote is encrypted but only the "sum" is decrypted .

### *4.1.1.2. Multiplicative Homomorphic Encryption schemes*

If an encryption algorithm E() is said to be multiplicative homomorphic, then it support multiplicative operations on encrypted data without the decryption of individual data's :

Enc (x□y) = Enc(x) * Enc(y)

Exemple (RSA cryptosystem) :



**Key Generation:** KeyGen$(p, q)$
**Input:** $p, q \in \mathbb{P}$
Compute $n = p \cdot q$
$\varphi(n) = (p-1)(q-1)$
Choose $e$ such that $\gcd(e, \varphi(n)) = 1$
Determine $d$ such that $e \cdot d \equiv 1 \bmod \varphi(n)$
**Output:** $(pk, sk)$
public key: $pk = (e, n)$
secret key: $sk = (d)$

**Encryption:** Enc$(m, pk)$
**Input:** $m \in \mathbb{Z}_n$
Compute $c = m^e \bmod n$
**Output:** $c \in \mathbb{Z}_n$

**Decryption:** Dec$(c, sk)$
**Input:** $c \in \mathbb{Z}_n$
Compute $m = c^d \bmod n$
**Output:** $m \in \mathbb{Z}_n$

*Figure 2: RSA cryptosystem*

If the RSA public key is modulus $m$ and exponent $e$, then the encryption of a message $x$ is given by $\mathcal{E}(x) = x^e \bmod m$.

The homomorphic property is then: $\mathcal{E}(x_1)\cdot\mathcal{E}(x_2) = x_1^e x_2^e \bmod m = (x_1x_2)^e \bmod m = \mathcal{E}(x_1 \cdot x_2)$

So, RSA cryptosystem realize the properties of the multiplicative Homomorphic encryption.

### 4.1.2. Fully homomorphic encryption

Fully homomorphic encryption includes two basic homomorphism types. They are the multiply homomorphic encryption algorithm and additively homomorphic encryption algorithm .The first FHE scheme was solved by Gentry [24,25] ,it's proceeds in three steps :

1) Constructs a Somewhat Homomorphic Encryption (SHE) scheme, namely which is able to decrypt correctly only a limited number of operations.
2) Express the encryption function by a low-degree polynomial (squash).
3) Applies the bootstrapping to reduce the noise and to compact the ciphertext.

More recently, two further fully homomorphic schemes were presented:

Van Dijk, Gentry, Halevi and Vaikuntanathan's (DGHV) scheme over the integers [12], based on the approximate GCD problem, and implemented in [13]. A batch version of this scheme has been proposed in [11].

Brakerski and Vaikuntanathan's (BV) scheme based on the Learning with Errors (LWE) problem [14] or Ring Learning with Errors (RLWE) problem [15]. Other implementations are in [16,17,18].

For simply, we use a symmetrical fully encryption homomorphic algorithm proposed by Craig Gentry [19]. Encryption algorithm The encryption parameters p, q and r, where p is a positive odd number, q is a large positive integer, p and q determined in the key generation phase, p is an encryption key, and r is a random number encrypted when selected. For the text m, calculation :

Encryption : $C=m+2r+pq$

Decryption : $M = (c \bmod p) \bmod 2$

Because the p*q is much less than 2r + m , then $(c \bmod p) \bmod 2=(2r + m) \bmod 2=m$

Homomorphism Verification [20] :

The homomorphism additive property verification: Suppose there are two groups of the plaintext m1 and m2. To encrypt them become the ciphertext.

$C1=m1+2\, r1+ pq1$ and $C2=m2+ 2\, r2+ pq2$

$C1+C2= m1+2\, r1+pq1 + m2+ 2\, r2+pq2= (m1+m2) +2(r1+r2) + p(q1+q2)$

As long as the (m1+m2) +2(r1+r2) is much less than[21], then: This algorithm satisfies the additive homomorphic conditions

The homomorphic multiplicative property verification :

$C1*C2= (m1+2r1+pq1)*(m2+2r2+pq2) = m1m2 + 2(2r1r2+r1m2+r2m1) + p [pq1q2+q2(m1+2r1) + q1(m2+2r2)]$

As long as the m1m2 + 2(2r1r2+r1m2+r2m1) is much less than, then This algorithm satisfies the multiplicative homomorphic conditions [22]

## 5. OUR APPROACH : A NEW FRAMEWORK TO ENHANCE DATA SECURITY IN THE CLOUD

Our approach consist in designing and implementing a framework using traditional encryption schemes(symmetric ,asymmetric ) and homomorphic encryption schemes( SHE and FHE) ,and we Integrate it to OpenStack cloud environment .The basic idea of this approach is giving to the Customer the possibility of choosing the type of encryption schemes according to the level of sensitivity of its data. But ,First he must do a classification of all its data (fig[3])

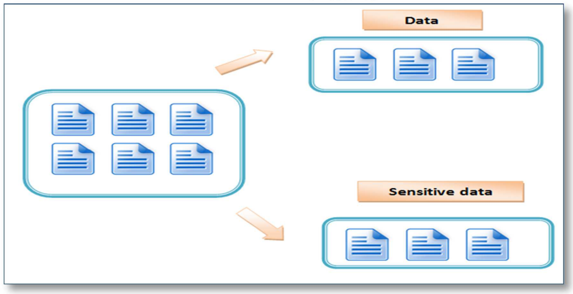


*Figure 3 : Classification of the data*

Then ,he choose one of the two options of the framework (security level 1 or 2) as shown in figure [4],

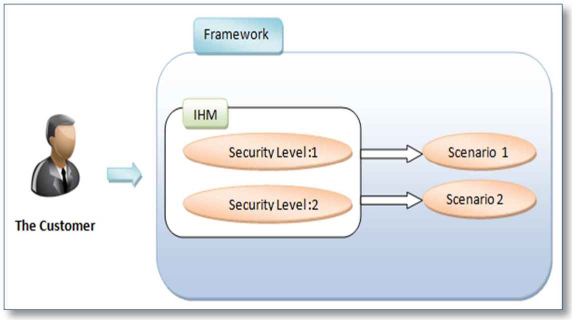


*Figure 4 : Design of the framework*

If he choose the first level of security so it's means that the encryption of his data will be with a fully homomorphic encryption scheme. The customer push his data to the cloud , which can perform arithmetic operations on it . He would like that the cloud provider know as little as possible about his data, and about the results of the computations. So he can store a encrypted data in the remote server using a fully homomorphic cryptosystem. The cloud computes the result which is an encrypted data too and sends the answer back to him. When the customer decrypt the result of his computation, then he should get back the plain text version of the result. In the figure [5] , we explain the principle :

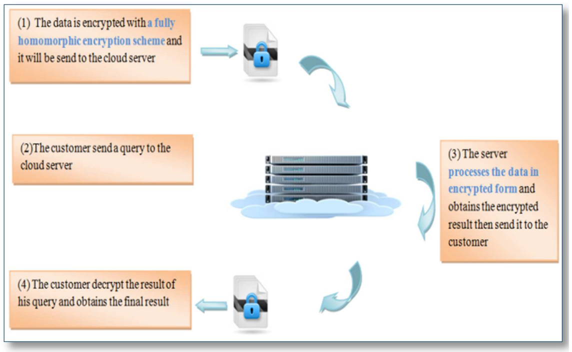

(1) The data is encrypted with a fully homomorphic encryption scheme and it will be send to the cloud server
(2)The customer send a query to the cloud server
(3) The server processes the data in encrypted form and obtains the encrypted result then send it to the customer
(4) The customer decrypt the result of his query and obtains the final result

*Figure 5: Data security scheme using a Fully Homomorphic Cryptosystem for cloud computing*

Else ,he choose the second scenario which means that the customer will use a traditional encryption scheme for his data, so the cloud provider can decrypt his data with the private key of the customer, then applies the query and send the result to the customer as shown in figure [6] :

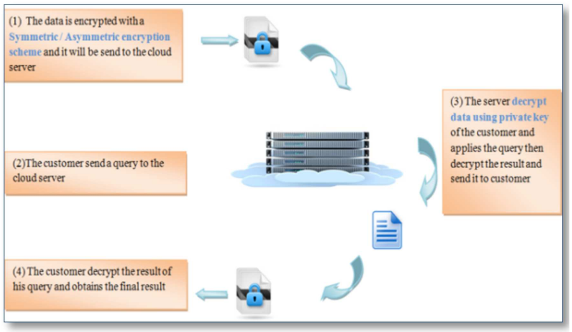

(1) The data is encrypted with a Symmetric / Asymmetric encryption scheme and it will be send to the cloud server
(2)The customer send a query to the cloud server
(3) The server decrypt data using private key of the customer and applies the query then decrypt the result and send it to customer
(4) The customer decrypt the result of his query and obtains the final result

*Figure 6 : Data security scheme using a Traditional Cryptosystem for cloud computing*

## 6. CONCLUSION

To summarize, Data security has become the most important issue of cloud computing security. The FHE represents a big step in modern cryptography and opens new challenges to cryptology researchers and also it helps the new IT technologies to be faster adopted. It is a new view of data security solution with encryption, which is important and can be used as reference for designing the complete security solution. In this paper we have survey on various encryption schemes ,Our futur work will be based on the application of traditional and fully Homomorphic encryption schemes to a Cloud environment , Analyze and improve the existing cryptosystem to allow servers to perform various operations requested by the client using openstack cloud .

## REFERENCES:

[1] Peter Mell, Tim Grance, The NIST Definition of Cloud Computing, Version 15, October 7, 2009,<URL:http://csrc.nist.gov/groups/SNS/cloud-computing>.

[2] Cisco Cloud Computing -Data Center Strategy, Architecture, and Solutions Point of View White Paper for U.S. PublicSector1st Edition

[3] http://www.cleverlogic.net/articles/cloud-computing-security-issues-and-solutions

[4] Cloud Security Alliance, Top Threats Working Group, “The notorious nine: cloud computing top threats in 2013”. February 2013.

[5] Peng, T., C. Leckie, and K. Ramamohanarao, Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys (CSUR), 2007. 39(1): p. 3.

[6] Subashini, S. and V. Kavitha, A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 2011. 34(1): p. 1-11.

[7] Rocha, F., and Correia, M. Lucy in the sky without diamonds: Stealing confidential data in the cloud. In Proceedings of the 1st International Workshop on Dependability of Clouds, Data Centers and Virtual Computing Environments (DCDV, with DSN’11) (June2011).

[8] A. Singh and M. Shrivastava, “Overview of Attacks on Cloud Computing” IJEIT, Vol. 1, Issue 4, pp. 321 323, April 2012.

[9] R.L.Krutz and R.D.Vines, ―Cloud Computing Software Security Fundamentals‖in Cloud Security: A Comprehensive Guide to Secure Cloud Computing‖, New York City, NY, Wiley, 2010

[10] R. Rivest, L. Adleman, and M. Dertouzos, ―On data banks and privacy homomorphisms,‖ in Foundations of Secure Computation ,Academic Press, 1978, pp. 169–177.

[11] J. H. Cheon, J.-S. Coron, J. Kim, M. S. Lee, T. Lepoint, M. Tibouchi, and A. Yun, Batch fully homomorphic encryption over the integers, Advances in Cryptology{EUROCRYPT 2013, Springer, 2013, pp. 315- 335.

[12] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, Fully homomorphic encryption over the integers, Advances in cryptology| EUROCRYPT 2010, Lecture

Notes in Comput. Sci., vol. 6110, Springer, Berlin, 2010, pp. 24-43.

[13] J.-S. Coron, A. Mandal, D. Naccache, and M. Tibouchi, Fully homomorphic encryption over the integers with shorter public keys, Advances in cryptology|CRYPTO 2011, Lecture Notes in Comput. Sci., vol. 6841, Springer, Heidelberg, 2011, pp. 487-504.

[14] Z. Brakerski and V. Vaikuntanathan, E_cient fully homomorphic encryption from (standard) LWE, 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science|FOCS 2011, IEEE Computer Soc., Los Alamitos, CA, 2011, pp. 97-106.

[15] Z. Brakerski and V. Vaikuntanathan, Fully homomorphic encryption from ring-LWE and security for key dependent messages, Advances in cryptology|CRYPTO 2011, Lecture Notes in Comput. Sci., vol. 6841, Springer, Heidelberg, 2011, pp. 505-524.

[16] M. Naehrig, K. Lauter, and V. Vaikuntanathan, Can homomorphic encryption be practical?, Proceedings of the 3rd ACM workshop on Cloud computing security workshop, ACM, 2011, pp. 113-124.

[17] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, (Leveled) fully homomorphic encryption without bootstrapping, Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, ACM, 2012, pp. 309-325.

[18] C. Gentry, S. Halevi, and N. P. Smart, Fully homomorphic encryption with polylog overhead, Advances in cryptology|EUROCRYPT 2012, Lecture Notes in Comput. Sci., vol. 7237, Springer, Heidelberg, 2012, pp. 465-482.

[19] GENS F. IT cloud services user survey, pt.2: top benefits & challenges[EB/OL]. http://blogs.idc.com/ie/?p=210, 2012-12-01.

[20] Feng Zhao ,Chao Li ,Chun Feng Liu , A cloud computing security solution based on fully homomorphic encryption ,

[21] Wikipedia.2009 Sidekick data loss [EB/OL]. http://en.wikipedia.org/wiki/ 2009_Sidekick_data_loss, 2012-12-0

[22] SONEHARA N, ECHIZEN I, WOHLGEMUTH S. Isolation in cloud computing and Privacy-Enhancing technologies[J]. Business & Information Systems Engineering, 2011, 3(3), 155-162.

[23] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In Eurocrypt 99, LNCS 1592, pages 223–238, 1999.

[24] C. Gentry, A fully homomorphic encryption scheme, Ph.D. thesis, Stanford University, 2009.

[25] Computing arbitrary functions of encrypted data, Commun. ACM 53 (2010), no. 3, 97-105.

[26] Jain, Nitin, Saibal K. Pal, and Dhananjay K. Upadhyay. "Implementation And Analysis Of Homomorphic Encryption Schemes." International Journal on Cryptography and Information Security (IJCIS) 2.2 (2012).