ANALYSIS OF HOMOMORPHIC ENCRYPTION SCHEMES AND ALGORITHMS FOR DATA SECURITY IN CLOUD COMPUTING

Sumitha.J [1], *Dr. S. Manju Priya* [2]

ABSTRACT

Now a days cloud computing plays an important role in internet era which is due to the mobile computing applications of cloud computing which becomes more important. Cloud Computing could be a quickly growing technology and it offers on-line accessible resources to the users.

By globally the infrastructure is moving towards the cloud computing technology. The cloud computing offers a service of third party authorization to demand services with rapid growth of technology and flexibility over the network.

Making certain that the safety of cloud computing is that the difficult issue within the cloud environments. It's a utility to deliver services and resources to the users through the high speed of net.

Keywords *:* Cloud computing, Cryptography, Homomorphic Encryption.

1. INTRODUCTION

A. Cloud Computing

It is the delivery of computing. By using the cloud, the client can just simply access the information at anytime, anywhere without the need of any special software. Cloud computing is having the benefits of space, efficiency and centralized large computational power. Cloud is nothing but a group of servers and data centres that are placed at different places and these are Responsible for providing on demand service to its users with the help of internet is shown in the Figure 1.

Fig.1: CLOUD COMPUTING [16]

Commonly data encryption techniques are used by clients to secure data on cloud computing. Generally if the client wants to apply some computational on his own data from the cloud on cloud storage, first of all he should retrieve the data by decrypting the cipher text from the cloud. After decryption he can apply the computation operations on that data, after applying operations client can again encrypt the result and store it on the cloud. So to avoid this long procedure of decrypting a data again and again the Homomorphic encryption method is used.

2. CLOUD DEPLOYMENT MODELS

Cloud computing is developed in four readying models specifically as shown in Fig 2.

[1] Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore

[2] Associate Professor, Department of CS, CA & IT Karpagam Academy of Higher Education, Coimbatore

Private cloud conjointly known as internal cloud that is been operated by a private organization. It managed by Amazon Elastic Cloud (EC2) or straightforward Storage Service (S3)

Public cloud permits systems and services to be simply accessible to general public. The IT giants like Google, Amazon and Microsoft supply cloud services via web. The resources could also be created out there freely or by pay- per-usage model.

Community cloud lies between the personal and public cloud. It's managed by all the collaborating organizations or by the third party. It shares the infrastructure between many organizations over specific community.

Hybrid cloud includes two or a lot of clouds. It's a combination of public and personal cloud.

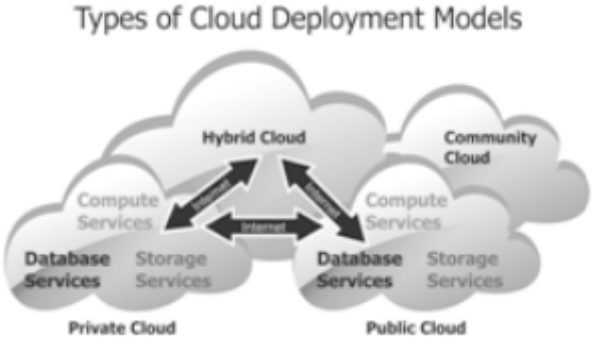

Fig.2: CLOUD DEPLOYMENT MODEL

3. SECURITY OF CLOUD COMPUTING

There are some security issues in cloud computing such as data security, third party control and privacy. It refers to a broad set of technologies and therefore the infrastructure of cloud computing.

But without the security of data in cloud, unauthorized users can access the data that results in great loss of customer.

The 3 needs of knowledge security area unit information Confidentiality, information Integrity, and information convenience. There is a way to perform operations on encrypted data on cloud server which is known as Homomorphic Encryption.

4. HOMOMORPHICENCRYPTION (HE)

Homomorphic coding performs coding on the encrypted information that is within the cloud.

It performs operations on the encrypted info and additionally the resultant is keep at intervals the cloud, thus none of them is alert to what exactly the knowledge is.

The homomorphic coding schemes are often classified per the operation that permits assessing on information, because the additivehomomorphic coding and increasing homomorphic coding.

Additive homomorphic coding schemes area unit schemes during which the cipher texts area unit computed because of add of plain texts.

In mathematics homomorphic encryption means conversion of one data set to another [2].

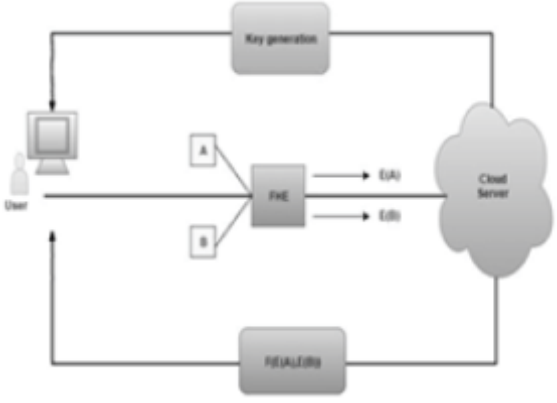

Fig.3: MECHANISM OF HOMOMORPHIC ENCRYPTION [1]

5. HOMOMORPHIC ENCRYPTION

The major operation of the Homomorphic Encryption is as follows [14]:

1) Key generation : The client generates the public key (pk) and the secret key (sk).

2) Encryption : The client encrypts the data with encryption key. It sends the encrypted data and pk to the Cloud server.

3) Request : The client sends a request to the server to perform operations on encrypted data.

4) Decryption : The client decrypts the returned result, using sk.

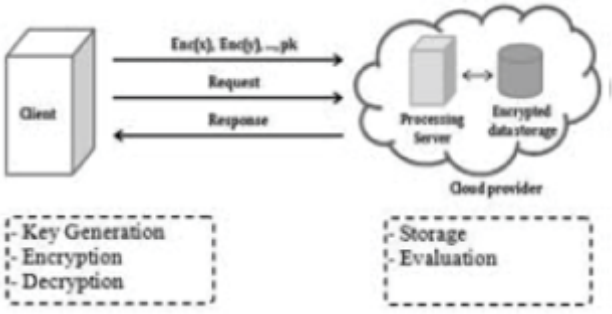

Fig.4: HE FUNCTIONS [11]

Depending up on the operations that are performed on Homomorphic encryption data it is categorized into three types namely:

1. Somewhat Homomorphic Encryption (SWHE)
2. Partially Homomorphic Encryption (PHE)
3. Fully Homomorphic Encryption (FHE)

SOMEWHAT HOMOMORPHIC ENCRYPTION (SWHE)

A somewhat homomorphic scheme (SWHE) is associate in secretly writing a scheme that is boots trappable with regards to a universal set of gates. The primary step is to style a theme that supports some computations over the encrypted knowledge.

Gentry has showed that if you're able to manage the look of SHE scheme that supports the analysis of its own secret writing algorithmic rule, then it's a general technique to rework the SHE theme into a FHE scheme.

The SHE uses low polynomial degree of cryptography that is claimed to be a main disadvantage.

A she will be able to value its own coding algorithmic program homomorphically is termed Bootstrappable and this kind of technique that transforms a boots trappable SHE theme into a FHE theme is thought as Bootstrapping.

PARTIALLY ENCRYPTION SCHEME

It is also called as "probabilistic asymmetric key algorithm" for public key cryptography this is often owing to the encoding of an equivalent plaintext under the same key gives as output a different cipher text [13].It performs operation on a single encrypted data.

(i) Unpadded RSA

If the RSA public key is modulus m and exponent e, then the encryption of a message is given by $\varepsilon(x) = x^e \bmod m$. The Homomorphic property is then

$\varepsilon(x1).\varepsilon(x2) = x1$

$ex2$

$e \bmod m = (x1x2)e \bmod m = \varepsilon(x1.x2)$ [8]

(ii) ElGamal

It is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key Exchange. Its encryption consists of three components [8]:

1. The key generator
2. The encryption algorithm
3. The decryption algorithm.

It is not securing under chosen cipher text attack and it gives a single plaintext that can be encrypted to many possible cipher texts.

(iii) Goldwasser-Micali

GM has the distinction of being the first probabilistic public key encryption scheme which is provably secure under standard cryptographic assumptions. [8] GM consists of three algorithms :

1. A probabilistic key generation algorithm which produces a public and a private key.
2. A probabilistic encryption algorithm.
3. A deterministic decryption algorithm.

The scheme relies on deciding whether a given value x is a square mod N, given the factorization (p, q) of N. [10]

This can accomplished using the following procedure:

1. Compute xp = x mod p, xq = x mod q.

2. If xp

(P-1)/2 = 1(mod p) and xq

(q--1)/2 = 1(mod q)

Benaloh Cryptosystem

It is created in the year of 1994. In GM each bit is encrypted individually. Benaloh, longer blocks of data can be encrypted at once. This scheme works in the group (Z/nZ)* where n is a product of two large primes [10].

Fully Homomorphic Encryption (FHE)

A cryptosystem that supports arbitrary computation on cipher texts is known as fully homomorphic encryption (FHE) [13].It is considered as ring homomorphism.

In June 2009, "Gentry" proposed the first efficient Fully Homomorphic Encryption technique. It is the sense of all algorithms run in polynomial time only.

A cryptosystem supports' arbitrary' computation on a cipher texts which is known as fully homomorphic encryption (FHE). In such a scheme it enables the programs for any functionality, which will run on encrypted inputs to produce an encryption of a result.

Fully homomorphic Encryption schemes are Craig Gentry scheme and Zaryab Khan Scheme. It performs both the addition and multiplication of computations.

6. COMPARISON TABLE OF TYPES OF HOMOMORPHIC ENCRYPTION

In Table 1, a comparison of some of the applications methods are executed in encrypted data without decrypting them.

Parameter	Partial HE	Fully HE
Type of operation supported in homomorphic encryption	It allows either addition or multiplication scheme	It allows both addition and multiplication operations
Computational limitations	It allows a limited number of computations	It allows a unlimited number of computations
Performance	It is faster and more compact	It has slower performance
Cipher text size	Its cipher text is small	Its cipher text is large

TABLE 1: COMPARISON OF PARTIAL AND FULLY HE [15].

In Table 2, a comparison of some of the Homomorphic properties with their respective schemes.

Scheme	Homomorphic properties	Type of Algorithm(Symmetric/ Asymmetric)
RSA	Multiplicative	Asymmetric
EIGamal	Multiplicative	Asymmetric
Goldwasse rMicali	XOR	Asymmetric
Benaloh	Additive	symmetric
Paillier	Additive	Asymmetric

TABLE 2: COMPARISON OF HOMOMORPHIC PROPERTIES [15].

7. CONCLUSION :

In this paper, a survey on Homomorphic encryption algorithms has been analysed.

The application of different Homomorphic Encryption cryptosystems such as (RSA, Paillier, ElGamal, Goldwasser-Micali, Boneh-Goh-Nissim and Gentry) on a Cloud Computing platform.

They are compared with four supported characteristics like: Homomorphic, cryptography, Privacy of Information, Security applied to them and also the keys that is been used.

Further the enhancements of analysing the behaviour of Homomorphic coding are compared to the length of the general public key and the time of the request by the Cloud provider hoping on the size of the encrypted messages.

REFERENCES :

1. V. Biksham, D. Vasumathi "Homomorphic Encryption Techniques for securing Data in Cloud Computing: A Survey", International Journal of Computer Applications Vol.160, February 2017.
2. T.Ramaporkalai, "Security Algorithms in Cloud Computing", International Journal of Computer Science Trends and Technology Vol. 5. Issue 2, Mar - Apr 2017.
3. Yasmina BENSITEL, Rahal ROMADI, "Secure data storage in the cloud with homomorphic Encryption", IEEE 2016.
4. Ryan Hayward, Chia-Chu Chiang, "Parallelizing Fully Homomorphic Encryption", IEEE, 2014.
5. Dr. Mohammad Miyan, "FHE Implementation of Data in Cloud Computing", International Journal of Advanced Research in Computer Science, Vol. 8, No. 3, March - April, 2017.
6. Kamal Kumar Chauhan, Amit K.S.Sanger, Ajai Verma, "Homomorphic Encryption for Data Security in Cloud Computing", IEEE 2015.

7. Zhaoe Min, Geng Yang and Jingqi Shi, "A privacy-preserving parallel and homomorphic encryption scheme", open Phys.2017.

8. Ramandeep Kaur1, Ashish Verma2, "A Review on Encryption Techniques to Secure cloud", International Journal of Science and Research, ISSN (Online): 2319-7064.

9. Prashant.K1, Ms. Ranjana.N2, "Secure Parallel Processing on Encryption Cloud Data Using Fully Homomorphic Encryption", International Journal of Computer Science and Mobile Computing, Vol.6 Issue.7, July- 2017.

10. www.wikipedia.org/wiki/Homomorphic_ encryption#Fully_homomorphic_encryption.

11. Khalid EL MAKKAOUI*, Abdellah EZZATI, Abderrahim BENI HSSANE,"Challenges of using Homomorphic Encryption to secure cloud computing", 2015 IEEE.

12. Mohd Rahul, Hesham A. Alhumyani, Mohd Muntjir, Minakshi Kambojl, "An Improved Homomorphic Encryption for Secure Cloud Data Storage", International Journal of Advanced Computer, Science and Applications, vol.8. No. 12, 2017.

13. D.Chandravathi, Dr.P.V.Lakshmi,"A new hybrid homomorphic encryption scheme for cloud data security," Advances in Computational Sciences and Technology, vol.10, 2017, pp.825-837.

14. Maha TEBAA, Said EL HAJII, "Cloud Computing through Homomorphic Encryption", International Journal of Advancements (IJACT), Vol. 8, No. 3, March - April 2017.

15. Shambhu Kumar Singh, Diksha R. Gupta, Ajay, R.Surse, "Homomorphic Encryption Technique for Storage of data on Cloud", international journal of science, spirituality, business and technology, vol. 4, no. 2, may 2016.