# **APPLICATION OF HOMOMORPHIC ENCRYPTION IN CLOUD SECURITY SYSTEM**

## **Contents**

### Chapter 1

### INTRODUCTION –

The concept of cloud computing and its growing attention in the IT industry and among users of cloud services have allowed individuals, organisations and third party1 cloud service providers to use software and hardware resources that are managed by virtualised6 technologythrough the internet space and at unknown remote locations. This has created a deep barrier, absence of understanding and some sense of insecurity between the clients and cloud services providers in area of data and information security for stored/processing data. This is so because of absence or non-existence of physical location of data centres for cloud computing.

Cloud computing enables users to get almost unlimited computing power, it provide instant availability, flexible and resource sharing capabilities with its virtualization2. Examples of cloud services offers by cloud providers include online file storage (e.g. Dropbox), social networking sites (e.g. Facebook), webmail (e.g. Gmail), and online business application (e.g. Brokerage).

Cloud computing allows sharing of information without users investing too much money in under-used resources, in cloud computing one can access data and information remotely that is stored on a server (e.g. Google Drive, Dropbox, iCloud) at any given time or location just by having access to the cloud service center through the internet.

Cloud computing have some essential characteristics which makes it services available any time and at any given location, these characteristics of cloud computing includes:

* *on-demand self-service*,
* *broad network* *access*,
* *resource pooling*,
* *rapid elasticity* and
* *Measured service*.

([P. Mell, 2011](#_ENREF_8)).

Although, cloud computing has now become wildly and most accepted way of computing by many organisation because of its cost effectiveness, scalability, elasticity and flexibility. It has also drawn very high concerns about the loss of privacy of their private data (security). In our Information communication technology (ICT) driven world today, there is the challenge of growing data storage and even processing whose obvious solution is cloud computing but, the storage and current technologies of also processing data and information on remote servers(cloud) rather than in-house has created some level of security fear to cloud clients and users.

The worry has been that having critical data reside outside the physical and virtual walls of the insurance enterprise (third party cloud) is a risky situation. As the IT field is rapidly moving towards Cloud Computing, software industry’s focus is shifting from developing applications for PCs to Data Centres and Clouds that enable millions of users to make use of software simultaneously.

“Attempting computation on sensitive data stored on shared servers leaves that data exposed in ways that traditional encryption techniques can't protect against,” ([Bhabendu Kumar Mohanta, 2013](#_ENREF_2)) .

Encryption of data could solve this. In traditional encryption, the main problem is that to manipulate an encrypted (cipher) data, the data has to be decoded (decipher) first, this scheme creates a vulnerability window and possible man-in-the middle attack. In traditional encryptions\*\*\* if the clients want to manipulate their encrypted data in the cloud, they have to share the secret key with cloud provider to decrypt it before execute the required operations ([K. Lauter, 2011](#_ENREF_5)),which is the current practice of data stored in cloud.

This work “APPLICATION OF HOMOMORPHIC ENCRYPTION IN CLOUD SECURITY SYSTEM”, demonstrate the theoretical and practical application of Homomorphic encryption to data security. Sometimes also called Fully Homomorphic Encryption (FHE), FHE performs computation on encrypted data without decrypting such data and send the encrypted data to the client and offers a realistic hope that such calculations can be performed securely in the cloud.

Homomorphic encryption is the appropriate solution to solve cloud computing security issues, since its schemes enable to perform computations on encrypted data without sharing the secret key needed to decrypt the data.

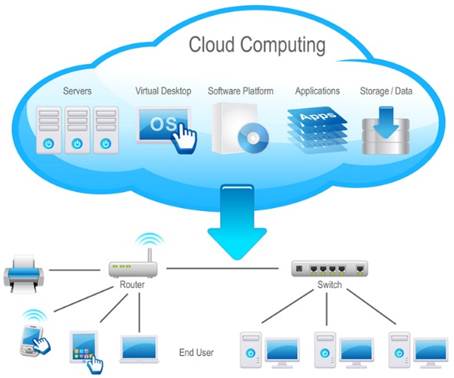
In 2009, Craig Gentry ([Gentry, 2010](#_ENREF_3)) introduced the first fully homomorphic encryption (FHE). In 2010, M. Dijk, C. Gentry et el. ([M. van Dijk, 2010](#_ENREF_6)) presented a second fully homomorphic encryption. In the march 2010, Gentry ([Gentry, 2010](#_ENREF_3)) proposed a homomorphic encryption scheme (called Gen10), heading toward widespread use of cloud computing. Unfortunately these schemes are insecure to use in cloud computing. In 2012, Jian Li, Danjie Song et al. ([J. Li, 2012](#_ENREF_4)) proposed a simple FHE derived from Gentry cryptosystem\*\*\* to ensure the privacy in cloud storage, namely SDC scheme. In 2014, Chen and Zhao ([Baohua Chen, 2014](#_ENREF_1)) proposed an improvement to the second scheme of Gentry to make the application of FHE in cloud is more secure.

Many researchers have proposed different applications of homomorphic encryption in cloud computing. In 2014, Yan Zhang et el. ([Yan Zhang, 2014](#_ENREF_10)) proposed a secure image retrieval method for cloud computing based on homomorphic properties of Paillier scheme. In 2015, Kocabas and Soyata ([Ovunc Kocabas, 2015](#_ENREF_7)) presented a method for privacy-preserving medical cloud computing using fully homomorphic encryption. In January 2016, Shu Qin Ren et el. ([Shu Qin Ren, 2016](#_ENREF_9)) proposed an XOR homomorphism encryption scheme to support secure keyword searching on encrypted data foe cloud storage.

This work seeks to addresses the security and confidentiality of student result and records in cloud computing for an educational institution (university of Abuja). The main aim of this work is to introduce the concepts of Homomorphic encryption and how to exploit the application of its concepts to secure cloud computing for educational records.

This work introduces and organized some fundamental concepts under the following sub headings as follows:

1. Describes the cloud computing concepts and its deployment and services models.
2. Discusses the security issues of cloud computing with related solutions.
3. provides the definition of homomorphic encryption and discusses some examples of existing homomorphic schemes.
4. describes how to use homomorphic encryption to secure cloud computing data of an educational institution (university of Abuja).



**Figure 1.** Cloud computing structure

### STATEMENT OF THE PROBLEM;

Cloud computing is the technology and choice for present and future day computing needs, it is offering cost-effective, on-demand and flexible way to optimise and achieve computing performance of data storing, processing, manipulation and transmitting information/data between clients (Cloud users) and data centre (cloud service1) . However, this technology has posed a security threat in the confidentiality, integrity and availability (CIA) of information in its custody because of its vatualisation2 technology.

The security threat pose by cloud computing are\* mainly in the areas of:

* Authentication of information in cloud centre for its clients.
* Information leakage through Partial encryption scheme (PES)\*\*\*3 which does not guaranty maximum security in clouds
* Men in the middle attack which could be initiated by insider/third party cloud service provider4 (untrusted providers).

### PURPOSE OF THE STUDY;

Encryption is the process of changing information in such a way as to make it unreadable by anyone except those possessing special knowledge or authority (usually referred to as a "key") that allows them to change the information back to its original, readable form. Encryption is used to protect our data. It protects our data when we entrust our personal, sensitive and important data to our computer system and in data centres. It also protects our valuable information: 'data-secrets' while being transmitted around the Internet. It protects our conversations, whether video, voice, or text. It protects our privacy. It protects our anonymity. And sometimes, it protects our lives.

This work is primary concern with providing an enhanced computer data algorithm (Encryption Algorithm) that protects our data from criminals, competitors, neighbours, family members and malicious attackers for not gaining access to our confidential information and to always maintain the integrity of all available data in our data centres (i.e cloud) to authorize user.

The Purpose of this study: application of homomorphic encryption in cloud security is to create a safe and secure computational mechanism for cloud computer using Homomorphic encryption algorithm scheme.

### SIGNIFICANCE OF THIS RESEARCH;

Homomorphic data encryption in cloud addresses traditional encryption schemes like the use of

* Username and password for authentication of records.
* RSA encryption scheme : encryption and subsequent decryption of stored data for possible operation(performing operation on decipher text)

With the above lapses of traditional encryption, there are possibility of client information on cloud to be accessed by a third party, intruder (man-in-the middle),SQL-injection etc to invade or even alter the privacy of client’s data there by compromising the confidentiality, integrity and availability of personal sored information on cloud.

The significance of this work: ‘Application of Homomorphic data encryption in cloud’, is to address, apply and demonstrate how efficient and effective Homomorphic encryption and its corresponding algorithm in cloud can be to enhance the security performance model for educational institution , for example university of Abuja records and data processing, accessing and storing system.

The use of traditional encryption schemes to encrypt remote data before sending to the cloud provider has been the most widely used technique for data security in cloud. In this method, client will need to provide the private key to the server to decrypt the data before perform the calculations required - there is a security gab in this traditional method. To bridge this gab, Homomorphic encryption allows to perform computations on encrypted data without decryption.

Other significant areas of this study include:

* **Personal**

This study is important because it allows every computer user (especially cloud computer users) to secure its data always and all times from unathurizesd person or agents to gain access.it protect personal information and guard against identity theft.

* **Business** and

This study is also highly significant to Business organisation who can use it to protect corporate secrets.

* **Governments**

This study can also be very helpful to governments who can use it to secure classified information and Espionage. Espionage uses encryption to securely protect folder contents, which could contain emails, chat histories, tax information, credit card numbers, or any other sensitive information. This way, even if your computer is stolen that data is safe.

### THE RESEARCH QUESTION/HYPOTHESIS

This work intends to critically examine the workings, operations and application of Homomorphic data encryption as a fundamental strong cloud security mechanism for cloud data operations.

The advantages of Homomorphic encryption techniques for processing encrypted data/ information in cloud without decrypting the stored cipher text for data manipulation and processing.

Investigate the possibility and propose the use of cloud computing with Homomorphic attribute scheme and properties in school/educational institution (university of Abuja) for its information management of students’ academic records.

The research sets of assumptions and questions will include**:**

#### Explain algorithms supporting Homomorphic encryption in cloud

#### Investigate and explain the security frame work, of Homomorphic encryption in data processing storing and retrieval.

#### Give an in-depth analysis of the security advantage of using Homomorphic encryption in cloud for authentication, encryption & privacy protection with fast data and information recover.

#### critically analyse

##### Homomorphic authentication technique for data accessing and encryption in our educational institutions (university of Abuja) student record and result processing.

##### Propose a model to implementing Homomorphic encryption for the result and records computation, storing and processing of school students record.

# Reference

## Diff Hellman key Exchange

The Diff Hellman key exchange is based on two protocols, which are:

-Set up protocol.

- Main protocol.

## Baohua Chen, N. Z. (2014). *Fully Homomorphic Encryption Application in Cloud Computing*. Paper presented at the 11th International Computer Conference

## Bhabendu Kumar Mohanta, D. G. (2013). Fully homomorphic encryption equating to cloud security: An approach. *IOSR Journal of Computer Engineering (IOSR-JCE)*

## *9*(2), 46-50.

## Gentry, C. (2010). Computing arbitrary functions of encrypted data. *Communications of The ACM, 53*(3), 97-105.

## J. Li, D. S., S. Chen, X. Lu. (2012). *A Simple Fully Homomorphic Encryption Scheme Available in Cloud Computing.* Paper presented at the Proceeding of IEEE.

## K. Lauter, M. N., V. Vaikuntanathan. (2011). Can Homomorphic Encryption be Practical *CCSW, 11*(Chicago, llinois, USA, ), pp. 113–124.

## M. van Dijk, C. G., S. Halevi, V. Vaikuntanathan, . (2010). Fully homomorphic encryption over the Integers. pages 24–43.

## Ovunc Kocabas, T. S. (2015). *Utilizing Homomorphic Encryption to Implement Secure and Private Medical Cloud Computing*. Paper presented at the 8th International Conference on Cloud Computing, IEEE.

## P. Mell, T. G. (2011). *The NIST Definition of Cloud Computing*. U. S. Department of Commerce: U. S. Department of Commerce.

## Shu Qin Ren, B. H. M. T., Sivaraman Sundaram, Taining Wang, Yibin Ng,Chang Victor, Khin Mi Mi Aung. (2016). Secure searching on cloud storage enhanced by homomorphic indexing.

## Yan Zhang, L. Z., Yuanfan Peng, Jing Zhang. (2014). *A secure Image Retrieval Method Based on Homomorphic Encryption for Cloud Computing.* Paper presented at the 19th International Conference on Digital Signal Processing.