Homomorphic Encryption- a Consolidate Element for Data Security in Cloud Computing

Nishigandha Lavkumar Dhotre, Rahul Ashok Chavan
Department of MCA, Mumbai University
Institute of Management and Computer Studies

***Abstract*--- Cloud computing is one of the emerging and fastest growing paradigms. It is a set of IT services that are provided to the customer over the network at low cost. It has many advantages which include efficiency, low cost, scalability and many more. This advantages of cloud computing resulted to rapid increase the use of cloud services. However, cloud computing presents an additional level of risk and other challenges. Privacy and security are the key issues for cloud storage. There are various risks which are related to the security in cloud but one of the major concerns is the security of data that is being stored on the cloud and privacy when the data is transmitted over cloud. Many methods have been introduced to overcome this issue. Encryption is one of them and widely used method to ensure the data confidentiality in cloud environment. This paper focus on cloud computing along with its various security and privacy issues and describing the role ofHomomorphic Encryption Scheme for ensuringthe data security with the help of cipher texts.**

***Keywords*---Cloud Computing, Data Security, Encryption,Homomorphic Encryption**

I. INTRODUCTION

The rapid growth in the degree of networks and connectivity with increasing amount of data has led many providers and data centres to build larger infrastructures for balancing the information. By replicating the data and distributing it across multiple servers on demand, useof resources has been improved significantly. Cloud computing is a type of computing that depends on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services such as servers, storage space and many other applications are provided to an organization's computers and devices through the Internet. Cloud computing has emerged as important paradigm that is use to store and maintain the data, software or many other resources over the internet .Various definitions and interpretations of "clouds" and / or "cloud computing" exist. In simple terms "Cloud computing is sharing of different resource and other computing services over the Internet". Cloud services allow customers and organization to use software, hardware and many other services that are managed by third parties at remote locations. Cloud computing is a type of service where user are offered with networked storage space and computer resources.

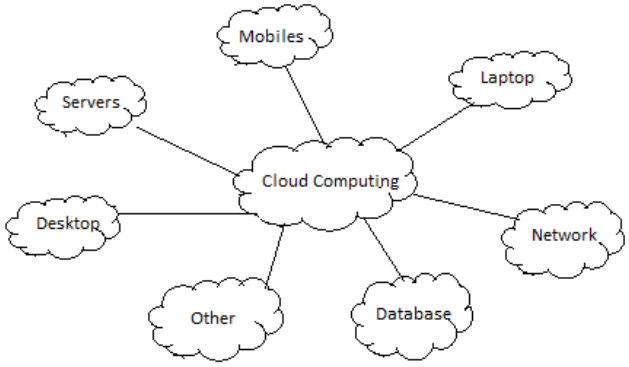


Figure 1: Cloud Computing

Examples of cloud computing services include networking sites, business applications and storage of file or other data on internet. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides shared resources,data storage space, networks, processing power, and other applications.

A. Characteristics of cloud computing:

Cloud computing provide rich set of services to the user that help them to use the services efficiently. Some of the cloud computing services are:

1) Self-Serve process: Services such as email, applications, network or server service can be provided without requiring human interaction with each service provider.

2) Distributed over large network: Cloud Capabilities are available over the large network and are accessed through standard mechanisms that are used by different client users such as mobile devices, laptops and other devices.

*3) Resource Sharing:*It enables provider's computing resources to pool together to serve multiple consumers and assigned according to consumer demand. The resources include among others storage, processing, memory, and other services.

4) Measuringusage of services: Cloud computing resource usage can be measured, controlled, and reported providing transparency for both the provider and consumer of the utilised service.

ISSN: 2278 – 1323

B. Deployment model:

To deploy the applications on the cloud, the users use three types of deployment model. They are:

*1) Public Cloud:*Public cloudis a type of deployment model thatoffersapplications, storage and other services to the general public. These services are made available to the public by a service provider.A public cloud is constructed to offer unlimited storage space and increased bandwidth via Internet. Publiccloud allows the customers to use the services on a low-cost, pay-as-you-gomodel.In Public cloud, infrastructure costs are spread across all users. One of the main advantageswhich come with using public cloud service is near unlimited scalability. Major concern related to public cloud is data security public cloud.

Figure 2: Deployment models of cloud[2]

2) Private Cloud: Private cloud is cloud infrastructure limitedfor a particular organization. It is not shared with other organizations. It is managed internally or by a third-party, or can exist internally or externally. The main advantage of a private cloud is the greater level of security offered making it ideal for users who need to store and/or process sensitive data. It is also more difficult to access the data held in a private cloud from remote locations due to the increased security measures.

3) Hybrid Cloud: Hybrid Clouds are a combination of two or more clouds (private or public) which are tied together offering the benefits of multiple deployment models. It is more scalable in terms that it contains both private and public cloud. It offers both secure and scalable public resources.

C. Service model:

Cloud computing offers three types of services as follows:

1) Infrastructure-as-a-Service (IaaS): Infrastructure-as-a-Service is the first layer. It is the foundation of cloud computing. Using this service model, you manage your, data, operating system and other applications. The service provider manages your servers, networking and storage.

Figure 4: Service models of cloud[2]

2) Platform-as-a-Service (PaaS): This cloud service model is the second layer. It manages your applications and data and the cloud vendor manages everything else. Benefits for using Platform-as-a-Service include ability to change and minimize expenses. One of the bestexamples of Platform-as-a-Service is the Google app engine.

3) Software-as-a-Service (SaaS): This is the final layer of the cloud services model. It is a software distribution model in which applications are hosted by service provider and made available to users over a network, typically the Internet.

D. Advantages of cloud computing:

1. The cloud is available at much cheaper rates which can lower the expenses. Also, it provides pay-as-you-go and other scalable options available, which make it very fair for the use.
2. Storing information in the cloud gives you almost unlimited storage capacity.
3. Since all the data is stored in the cloud, back-up and restore of the same is much easier than storing the same on a physical device.
4. In the cloud, Cloud users don't need to take additional efforts to customize and integrate their applications as per own preferences.
5. Once the users register in the cloud, they can access the information from anywhere, where there is an Internet connection.
6. Lastly and most importantly, Cloud computing gives the advantage of fast deployment.

E. Disadvantages of cloud computing:

1. Security is the biggest concern when it comes to cloud computing. Whenusing a remote cloud based infrastructure, theuser gives away his private and confidential data. It is then up to the cloud service provider to manage, protect and retain them. Similarly, privacy in the cloud is another huge issue. Users have to trust their cloud service provider that they will protect their data from unauthorized access.
2. One of the major disadvantages of cloud computing is the implicit dependency on the provider. This means that the user has to completely depend on the cloud provider for securing and also migrating from one provider to another becomes difficult.
3. As Cloud entire setup is dependent on internet access, any network or connectivity issuecan hinder the efficiency making it dysfunctional for some period of time.
4. When multiple users try to access or execute the same resources at same time, it can generally decrease the efficiency of the cloud and limit its usage.

ISSN: 2278 – 1323

II. DATA SECURITY ISSUES IN CLOUD COMPUTING:

Despite of the popularity of cloud computing, it is facing many difficulties. One such problem is security that is one of the major obstaclefor the growth of cloud computing. Data security is at the top of the list of security concern for cloud. Here are some of the key security challenges faced by the cloud:

1. *Data Location on cloud:*In general, the cloud users are not aware of the exact location where the data is stored. Also they do not have any control over the access to the stored data.

2. *Unwanted Access:*Cloud computing can actually increase the risk of access to confidentiality information. In general, cloud storage can be more at risk from malicious behaviour because the data in the cloud can be exposed as it is stored there for long time.

3. *Data Sharing:*Data in the cloud is typically in a shared environment together with data from other customer. Encryption cannot be only solution for data sharing problems. In some situation, user may not want to encrypt data because there may be chance of accidently destroying the data when performing encryption.

4. *Dependency on cloud vendor:*One of the major disadvantages of cloud computing is the implicit dependency on the provider. This means that the user has to completely trust the cloud provider for securing our data.

5. *Data Remanence:*Another important issue for cloud is how to be sure that the data once deleted from the cloud storage is not recoverable by the provider. There is no exact mechanism to ensure this. Also the problem extends as there can be multiple copies of same data stored at different location on the cloud.

III. ENCRYPTION TECHNIQUES

To secure data on the cloud storage the most efficient method is to encrypt the data. Different Cryptographic techniquescan be applied to data offer the best solution for data protection. These means that data should be first encrypted locally and then upload it to cloud.

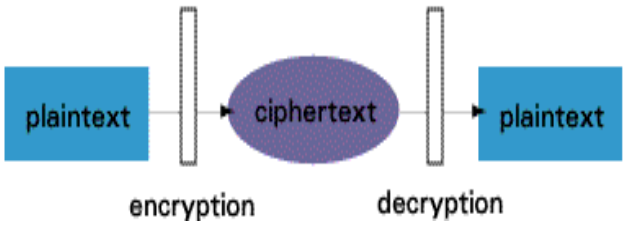


Figure 5: Basic Encryption and Decryption Process

A. Security Encryption Algorithms used in Cloud Computing:

Different security algorithms to eliminate the concerns regarding data loss, data sharing and privacy while accessing web application on cloud. Some of them are as follows:

1) RSA Algorithm

RSA algorithm is used to ensure the security of data in cloud computing. In this algorithm data is being encrypted to provide security. After encrypting, data is stored in the cloud. So that when it is required then a request can be placed to cloud provider. Cloud provider first authenticates the user and then delivers the data to user. RSA is a Block Cipher in which every message is mapped to an integer. In the proposed cloud environment, Public key is known to all, whereas Private Key known only to user who originally owns the data. Thus encryption process is carried out by the cloud service provider and decryption is done by the cloud user or consumer. Once the data is encrypted with the Public key, it will be decrypted using the corresponding Private Key only.

2) AES Algorithm

AES(Advanced Encryption Standard), is the encryption standard given by NIST. AES has variable key length of 128, 192, or 256 bits. The default length is 256. AES encrypts data blocks of 128 bits in 10, 12 and 14 round depending upon the size of the key. AES encryption technique is fast and flexible. AES has been carefully tested for many security applications.

3) DES Algorithm

The Data Encryption Standard (DES) is a block cipher. It encrypts data in blocks of size 64 bits each. That is 64 bits of plain text goes as input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length of this algorithm is 56 bits; however a 64 bits key is actually input. DES is therefore a symmetric key algorithm.

The above encryption algorithms are a well-known technique thatensures the security of sensitive information stored on the cloud. It is being used by many cloud computing applications. However these encryption mechanisms, has a drawback.When the data is stored on the cloud, it can be sent to and from in encrypted format resulting, the servers cannot do any operations on it. The system working with encrypted data can either, retrieve or store the data for the client. Any otherdifficult operations require that the data must be first decrypted. Thus increased in demand for enhanced security and inherent limits of traditional encryption schemes for data on the cloud has driven the adoption and implementation of new encryption technique known as Homomorphic Encryption.

ISSN: 2278 – 1323

IV. HOMOMORPHIC ENCRYPTION

An encryption scheme is "homomorphic" if it is possible to perform implicit operation on the plaintext by processing the ciphertext only. Homomorphic encryption is the encryption technique on the already encrypted data rather than on the original data that provide the result as it is done on the plain text. The complex mathematical operations can be performed on the cipher text without changing the nature of the encryption.

A. Why Homomorphic Encryption?

When the data stored at the Cloud we use standard encryption techniques to secure the operations and the storage of the data. The basic concept is to encrypt the data before it is send to the Cloud provider. But the disadvantage of these is that, one needs to decrypt data at every time he needs to perform operation on that data. For these purpose, client will need to provide the private key to the Cloud provider to decrypt data, which can affect the privacy of data stored in the Cloud.

Homomorphic Encryption proposes a method to operate on encrypted data without decrypting them. This method will provide the same results after calculations that had obtained if worked directly on the raw data. Homomorphic encryption converts data into cipher text that can be worked with as if it were still in its original form. Homomorphic encryptions allow complex operations to be performed on encrypted data without compromising the encryption. Homomorphic Encryption techniques are used to perform operations on encrypted data without knowing the private key i.e. without decryption.When decrypt the output of any operation is similar to the operation performed on the raw data.

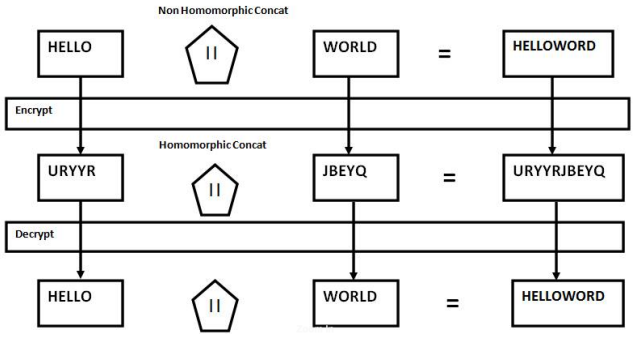


Figure 6: A string concat example of homomorphic encryption

B. Function of Homomorphic Encryption[6]:

Homomorphic Encryption H is a set of four functions:

H = {Key Generation, Encryption, Decryption, Evaluation}

1. Key generation: client will generate pair of keys public key pk and secret key sk for encryption of plaintext.

2. Encryption: Using secret key sk client encrypt the plain text PT and generate Esk (PT) and along with public key pk this cipher text CT will be sent to the server.

3. Evaluation: Server has a function f for doing evaluation of ciphertext CT and performed this as per the required function using pk.

4) Decryption: Generated Eval(f(PT)) will be decrypted by client using its sk and it gets the original result.

C. Properties of Homomorphic Encryption[6]:

1) Additive Homomorphic Encryption:

A Homomorphic encryption is additive, if:

$$Enc(a \oplus b) = Enc(a) \oplus Enc(b)$$

Suppose there are two ciphers C1 and C2 such that:

$$C1 = g^{m1} x_1^{\,n} \bmod n^2$$
$$C2 = g^{m2} x_2^{\,n} \bmod n^2$$

Therefore,

$$C1.C2 = g^{m1} x_1^{\,n} . g^{m2} x_2^{\,n} \bmod n^2$$

Additive Property is:

$$g^{m1+m2}(x_1 x_2)^n \bmod n^2$$

2) Multiplicative Homomorphic Encryption:

Homomorphic encryption is multiplicative, if:

$$Ek(PT1 \otimes PT2) = Ek(PT1) \otimes Ek(PT2)$$

Suppose there are two ciphers C1 and C2 such that:

$$C1 = m1^e \bmod n$$
$$C2 = m2^e \bmod n$$

Therefore,

$$C1.C2 = m1^e.m2^e \bmod n$$

So Multiplicative Property is:

$$(m1.m2)^e \bmod n$$

V. HOMOMORPHIC ENCRYPTION ALGORITHMS

A. Partial Homomorphic Encryption Schemes:

Under this section different partial homomorphic encryption techniques are being discussed:

1) RSA

RSA exhibits multiplicative homomorphism. By multiplying two (or more) RSA ciphertexts together, the decrypted result is equivalent to the multiplication of the two (or more) plaintext values.RSA has a multiplicative homomorphic property i.e., it is possible to find the product of the plain text by multiplying the cipher texts. The result of the operation will be the cipher text of the product.The homomorphism is:

Suppose there are two plaintexts P1 and P2. Then

$$ek(P1)\, ek(P2) = P1^b P2^b \bmod n$$
$$= (P1P2)^b \bmod n$$
$$= ek(P1P2)$$

ISSN: 2278 – 1323

Characteristics:

- It is multiplicative homomorphic encryption scheme.
- Provide secure communication.
- Different keys are used for encryption and decryption.
- Used to secure internet banking and credit card transactions.

2) Paillier

Paillier follows additive homomorphic encryption. By multiplying each component of multiple ciphertexts with their corresponding respective components, the decrypted result is equivalent to the addition of the plaintext values.

The Homomorphic: Suppose x_1 and x_2 are plaintext.

Then,

$$Ek(x_1,r_1).ek(x_2,r_2) = g^{x1} r_1^m g^{x2} r_2^m \bmod n^2$$
$$= g^{x1+x2}(r_1 r_2)^m \bmod n^2$$
$$= ek(x_1 + x_2, r_1 r_2)$$

Characteristics:

- It is additive homomorphic encryption scheme.
- Provides secure storage and communication.
- Similar to RSA, it also used different keys for encryption and decryption.
- It is mostly used in voting systems.

3) ElGamal

ElGamal exhibits multiplicative homomorphism. By multiplying each component of multiple ciphertexts with their corresponding respective components, the decrypted result is equivalent to the multiplication of the plaintext values. ElGamal also has a multiplicative homomorphic property.

Given ciphertexts (c1, c2) and (d1, d2) that are encryptions of m1 and m2, using random values $X_{B1}$and X_{B2}, respectively, then

$$(c1d1, c2d2) = (g^x_{B1} g^x_{B2}, (m1.S_1)\ (m2.S_2))$$
$$= (g^{x}_{B1\ +x_{B2}}, m1m2.S_1+S_2)$$

Characteristics:

- It is multiplicative homomorphic encryption scheme.
- It ensures secure communication and storage.
- It is mostly used for security in Hybrid systems.

The partial Homomorphic Encryption algorithms like ElGamal, RSA, Paillier are well proved in term of security therefore, one can consider these schemes for implementing practical applications. However, the partial homomorphic encryption schemes have some limitations, majority of these schemes **support only one type of operation**, therefore usage of these schemes in practical applications have big restriction, and most of the applications require more than one operation need to be performed.Therefore, these algorithms need to be used in combination with other algorithms as required by the applications.

B. Fully Homomorphic Encryption [7]:

Up until now, the homomorphic techniques described have been partially homomorphic. They all preserve the structures of either multiplication or division, but cannot do both.For all types of calculation on the data stored in the cloud, we must opt for the fully Homomorphic encryption which is able to execute all types of operations on encrypted data without decryption.

A cryptosystem which supports both addition and multiplication is known as fully homomorphic encryption (FHE) and is far more powerful. Using such a scheme, any circuit can be evaluated homomorphically, and effectively allowing the construction of programs which may be run on encryptions of their inputs to produce an encryption of their output. Since such a program never decrypts its input, it can be run by an untrusted party without revealing its inputs and internal state. The existence of an efficient and fully homomorphic cryptosystem will have great practical implications in the outsourcing of private computations, especially, in the context of cloud computing.

1) Gentry's Scheme[7]: In 2009, Gentry proposed first fully homomorphic encryption scheme. This was a great achievement in cryptographic research that eventually had huge implication in privacy and security. His proposed scheme consists of several steps:

a) It constructs a somewhat homomorphic scheme that supports evaluating low-degree polynomials on the encrypted data.

b) It squashes the decryption procedure so that it can be expressed as a low-degree polynomial which is supported by the scheme i.e. Modulus reduction procedure.

c) It applies a bootstrapping transformation to obtain a fully homomorphic scheme.

2) Smart and Vercauteren Scheme [7]: At 2010 Smart and Vercauteren made the first attempt to implement Gentry's scheme using a variant based on principal ideal lattices and requiring that the determinant of the lattice be a prime number.However the authors could not obtain a boots-trappable scheme because that would have required a lattice dimension of at least n = 227, whereas due to the prime determinant requirement they could not generate keys for dimensions n > 2048, which is essential for security purposes. This implied that Gentry's blueprint was not yet practical.

3) Gentry and Halevi Scheme [7]: In 2010, Gentry and Halevi presented a novel implementation approach for the variant of Smart and Vercauteren proposition which had a greatly improved key generation phase. In particular, key generation is essentially an application of a Discrete Fourier Transform (DFT), followed by a small quantum of computation, and then application of the inverse transform. The key generation method of Gentry and Halevi is fast.

C. Partial versus Fully Homomorphic Encryption:

Sr No.	Partial Homomorphic Scheme	Fully Homomorphic Scheme
1.	It allows either additive or multiplicative scheme	It allows both additive and multiplicative operations
2.	It follows for limited number of computation	It follows for an unlimited number of computation

ISSN: 2278 – 1323

3.	It do not support only one type of operation	It supports more complex operations.
4.	It requires less computational efforts	It requires more computational efforts
5.	It is faster in performance and more compact than fully homomorphic scheme.	It has slower performance as compare to Partial scheme

VI. IMPLEMENTATION:

Homomorphic encryption is expected to play an important part in cloud computing, allowing companies to store encrypted data in a public cloud and take advantage of the cloud provider's analytic services. Suppose we want to do computation on$\{m1, m2 \ldots mn\}$but want to utilize cloud server for the computation. Since we do not want to give cloud server access to data itself, homomorphic encryption method proves to be best option.The methodology adapted by these areas is discussed below:

Mechanism:

1. Client sends an encrypted data to cloud
   - Eg: let two encrypted number be a and b.

2. Client sends request to Cloud for calculating function
   - i.e. f(a,b)

3. Client and Cloud communicate through a cryptosystem based on fully homomorphic encryption.

4. Cloud stores encrypted data

5. Cloud calculates the result of request sent by the client without knowing actual number
   - i.e. f(a,b) is calculated

6. Cloud then compute f(Enc(a),Enc(b)) without knowing a and b

7. Client decrypts f(Enc(a),Enc(b)) using its private key.

Here is a very simple example of how a homomorphic encryption scheme might work in cloud computing:

Example:

Suppose Business A has a Data that consists of two numbers 1 and 2. To encrypt the data set, Business encrypts the data, creating a new set whose members are 33 and 54 respectively. Business A sends the encrypted data to the cloud for safe storage. A few months later, theother organization contacts Business A and requests the sum of data elements. Business A is busy, so it asks the cloud provider to perform the operation. The cloud provider, who only has access to the encrypted data set, finds the sum of 33 + 54 and returns the answer 87. Business A decrypts the cloud provider's reply and provides the government with the decrypted answer, 3

VII. BENEFITS OF HOMOMORPHIC ENCRYPTION TECHNIQUES

1) Solves Confidentiality problems: The homomorphic encryption solves the major confidentiality issue when different users want to perform operation on the data that needs to be shared among many users.

2) Ability to compute over ciphertext instead of plaintext: Homomorphic Encryption proposes a method to operate on encrypted data without decrypting them. This method will provide the same results after calculations that had obtained if worked directly on the raw data.

3) One could use information without knowing the content of that information: As homomorphic encryption operates on the encrypted data anyone can use that information without actually knowing the information.

4) Privacy guaranteed: Homomorphic Encryption guarantees data privacy as all the computation are carried out on the encrypted data. Complete privacy between client and server would be possible without any decreased functionality.

VIII. APPLICATION

1) Protection of mobile agents: One of the most interesting applications of homomorphic encryption is its use in protection of mobile agents. Since all older computer architectures are based on binary strings and only require multiplication and addition, homomorphic techniques would offer the possibility to encrypt the data. Hence, it could be used to protect mobile agents against malicious hosts by encrypting them.

2) Secret sharing scheme: In secret sharing schemes, parties share a secret. In some case, no other party can reconstruct the secret form the information available to it. But sometimes parties may be able to reconstruct the key. In this case, the homomorphic encryption techniques can be useful.

*3) Banking:*Suppose that a customer has the total value of their accounts encrypted using their private key and that is what is stored on the bank's servers. Without decrypting the customer's account values, things such as interest and transfers could theoretically be computed without ever needing to view the customer's specific dollar amount attached to their accounts.

4) Watermarking and fingerprinting schemes: Digital watermarking and fingerprinting schemes embed additional information into digital data. The homomorphic property is used to add a mark to previously encrypted data.

5) Data aggregation in wireless sensor networks: In-network data aggregation in WSNs is a technique that combines partial results at the intermediate nodes enroute to the base stationthereby reducing the communication overhead and optimizing the bandwidth utilization in the wireless links. Homomorphic encryption schemes can be

ISSN: 2278 – 1323

applied to protect privacy of input data while computing an arbitrary aggregation function in a wireless sensor network.

*7) Private Information retrieval:*One great application for homomorphic encryption is that of private information retrieval. This process could not discoverany data from the search engine but still providing meaningful information to the user. While the search engine is the mostly has such uses, process of retrieving the information could implement homomorphic encryption to protect a user's privacy.

X. CONCLUSION

Cloud computing is an emerging technology for the next generation of IT applications. The barrier toward the rapid growth of cloud computing are data security and privacy issues. A number of techniques have been proposed by researchers for data protection and to attain highest level of data security in the cloud. In this paper we have discussed some key data security issues and also different techniques to provide data security. In this paper we have given some fully homomorphic encryption scheme developed by researchers which allow us to perform computation on encrypted data without using secret key of client. It is nothing but a new layer applied to the cloud computation.

In future, we are going to work on the behaviour of Homomorphic Encryption Cryptosystems compared to the length of the public key and the performance of the request by the cloud provider that depends on the size of encrypted messages.

References:

[1] http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/Essential%20characteristics%20of%20Cloud%20Computing.pdf.

[2] http://www.appcore.com/3-types-cloud-service-models/

[3] Secure User Data in Cloud Computing Using Encryption Algorithms
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.377.8745&rep=rep1&type=pdf

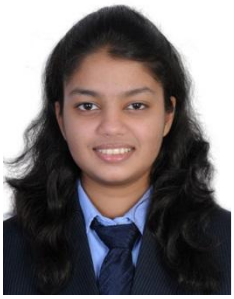
[4]Favored Encryption Techniques for Cloud Storage
http://www.researchgate.net/profile/Jerry_Gao/publication/273635294_Favored_Encryption_Techniques_and_Evaluation_for_Big_Data_in_a_Cloud/links/55123d0b0cf268a4aae9f096.pdf

[5].Secure Cloud Computing through Homomorphic Encryption
http://arxiv.org/ftp/arxiv/papers/1409/1409.0829.pdf

[6] Survey of Various Homomorphic Encryption algorithms and Schemes
http://research.ijcaonline.org/volume91/number8/pxc3895081.pdf

[7] Survey of Fully Homomorphic Encryption and Its Potential to Cloud Computing Securityhttp://www.ijarcsse.com/docs/papers/Volume_4/7_July2014/V4I7-0404.pdf

[8] Homomorphic Encryption: Theory & Applicationhttp://arxiv.org/ftp/arxiv/papers/1305/1305.5886.pdf



Nishigandha Lavkumar Dhotre
Pursuing Master of Computer Application (MCA) from Institute of Management & Computer Studies (IMCOST)
Thane

Rahul Ashok Chavan
Pursuing Master of Computer Application (MCA) from Institute of Management & Computer Studies (IMCOST)
Thane

ISSN: 2278 – 1323