ISSN (Online): 2349-7084

*International Journal of Computer Engineering In Research Trends (IJCERT)*
*Volume 1, Issue 2, August 2014, PP 77-82*
www.ijcert.org

# Intensification of Information safety by Cryptography in Cloud Computing

K.Sivanagalakshmi[1], M.Tech Research Scholar,
R.Anil Kumar[2], Assistant Professor,
Dr.S.Prem Kumar[3], Head of the Department

Department of CSE, G.Pullaiah College of Engineering and Technology, Kurnool
JNTU Anatapur, Andhra Pradesh, India

**Abstract**: *Cloud computing security challenges and it's additionally an issue to numerous analysts; first necessity was to concentrate on security which is the greatest concern of associations that are considering a move to the cloud. The points of interest of Cloud computing incorporate decreased expenses, simple upkeep and re-provisioning of assets, and consequently expanded benefits. Yet the appropriation and the section to the Cloud computing applies just if the security is guaranteed. Instructions to surety a finer information security furthermore in what manner would we be able to keep the customer private data secret? There are two real inquiries that present a test to Cloud computing suppliers. At the point when the information exchanged to the Cloud we utilize standard encryption routines to secure the operations and the stockpiling of the information. Anyhow to process information placed on a remote server, the Cloud suppliers need to get to the basic information. In this paper we are proposing Homomorphic encryption algorithm to execute operations on encoded information without decoding them which will give us the same comes about after computations as though we have worked straightforwardly on the basic information*

**Keywords:** Homomorphic Encryption, Cloud Computing, Cryptography, Information Security

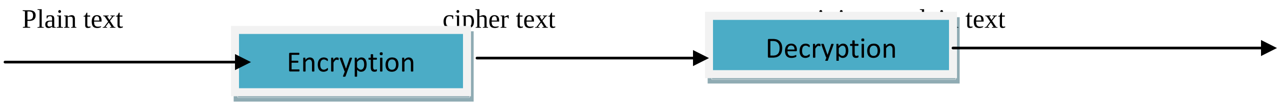
## 1. INTRODUCTION

Cloud computing is started off with Grid Computing, where large number of systems are used for solving scientific problem that require high levels of parallel computation. This technology expanded exceptionally, which eventually stimulated concerns over ensuring data security in public networks .According to a recent Survey conducted by Cisco Global Cloud Networking Academy, it has been revealed that 72 percent of IT professionals stated that security of data is a major hindrance to implement the services in cloud [1]. Recent development in cloud storage and the services rendered by it allows users to outsource storage. As a result, it allows companies or organizations to offload the task of maintaining datacenters. In the past few years, the security requirements for data are very strong and many algorithms have evolved [2]. Only a few algorithms play a comprehensive role in creating and maintaining a secure session over vulnerable public networks. Public key cryptography is one of the commonly used algorithms for this type of operation. The authenticity between the communicating parties is ensured by implementing this technique. These communicating parties share their private keys amongst them before exchanging information. In the case of transmitting a message over a public channel, the work of Diffie Helman [1] and RSA [3] provides way to encrypt a message into cipher text using private key. Consequently, the receiver on the other side has to read the cipher text by decryption with the help of their private key. The encryption scheme shows that the secret decryption key allows retrieving the actual text but if the secret key is lost, the cipher text is of no use. In 1978, RDA [4] decided to propose a technique on performing arbitrary computations on encrypted data. Such techniques give rise to useful applications to privately perform manipulations on encrypted data in the cloud. The necessary data can be decrypted by performing their corresponding computations. Assuring privacy tend to be very critical when complex computations are performed on encrypted data .Homomorphic encryption is evolved to solve such critical issues.

## 2. ENCRYPTION AND DECRYPTION

In cryptography, there are 2 basic styles of encoding schemes: Symmetric-key and public-key encoding. In symmetric-key schemes, the encoding and decipherment keys area unit an equivalent. Therefore communication parties should agree on a secret key before they want to speak. In public-key schemes, the encoding secret is printed for anyone to use and code messages. However, solely the receiving party has access to the decipherment key and is capable of reading the encrypted messages. Public-key encoding may be a comparatively recent invention: traditionally, all encoding schemes are symmetric-key (also referred to as private-key) schemes. Encryption, by itself, will defend the confidentiality of messages, however different techniques area unit still required guarding the integrity and believability of a message; for instance, verification of a message authentication codes (MAC) or a digital signature. Standards and crypto logical package and hardware to perform encoding area unit wide out there, however with success exploitation encoding to confirm security could also be a difficult drawback.

Encryption and decipherment area unit each strategy won't to make sure the secure passing of messages and different sensitive documents and knowledge. Encoding essentially suggests that to convert the message into code or disorganized kind, in order that anybody United Nations agency doesn't have the 'key' to unscramble the code, cannot read it. This is often sometimes done by employing a 'cipher'. A cipher may be a variety of algorithmic program employed in encoding that uses a precise delineate technique to scramble the information. The cipher will solely be 'deciphered' with a 'key'. A secret is the particular 'described method' that was wont to scramble the information, and thus the key may unscramble the information. Once the information is unscrambled by the employment of a key, that's what's called 'decryption'. It’s the other of encoding and also the 'described method' of scrambling is largely applied in reverse, thus on unscramble it. Hence, the hugger-mugger and unclear text becomes decipherable all over again.



Encryption with key: Encryption key: $K_E$ ; Decryption key: $K_D$ ;$C = E(K_E, P)$;$P = D(K_D, E(K_E, P))$

## 3. HOMOMORPHIC ENCRYPTION

Homomorphic cryptography permits access to extremely ascendable, cheap, on-demand computing resources which will execute the code and store the info that square measure provided to them. This facet, referred to as information outsourced computation is extremely engaging, because it alleviates most of the burden thereon services from the patron. All the same, the adoption of knowledge outsourced computation by business includes a major obstacle, since the info owner doesn't need to permit the international organization sure cloud supplier to own access to the info being outsourced. Simply encrypting the info before storing it on the cloud isn't a viable resolution, since encrypted information cannot be any manipulated? This implies that if data owner would love to go looking for explicit information, then the info would wish to be retrieved and decrypted a awfully expensive operation, that limits the usability of the cloud to simply be used as an information storage centre.

Homomorphic cryptography systems square measure accustomed perform operations on encrypted information while not knowing the personal key (without decryption), the consumer is that the solely holder of the key. After we decode the results of any operation, it's constant as if we tend to had meted out the calculation on the data.

**Definition:** associate cryptography is Homomorphic, if: from Enc (a) and Enc (b) it's doable to reason Enc (f (a, b)), wherever f will be: +, ×, ⊕ and while not exploitation the personal key.

For plain texts P1 and P2 and corresponding cipher text C1 and C2, a Homomorphic cryptography theme permits meaning computation of P1 ʘ P2 from C1 and C2 while not revealing P1 or P2.The cryptosystem is additive or increasing Homomorphic relying upon the operation ʘ which may be addition or multiplication.

A Homomorphic encryption system contains following four algorithms:

**KeyGen** (λ):

- Input-the security parameter λ.
- Output-a tuple (sk, pk) consisting of the secret key sk and public key pk .

**Encrypt** ( pk,π ):

- Input-a public key pk and a plaintext π .
- Output-cipher text Ψ.

**Decrypt** (sk ,Ψ ):

- Input-a private key pk and a cipher text Ψ .
- Output-the corresponding plaintext π .

**Evaluate** (pk ,C ,Ψ ):

- Input-a public key , a circuit with inputs and a set Ψ of cipher text ,Ψ1 . . . . . Ψt

Output-a cipher text Ψ.

Therefore, a Homomorphic encryption scheme consists of all algorithms of a conventional public key encryption scheme and an extra one. The correctness-condition for the conventional part of a Homomorphic encryption scheme is identical to that of a (non-Homomorphic) public key encryption scheme.

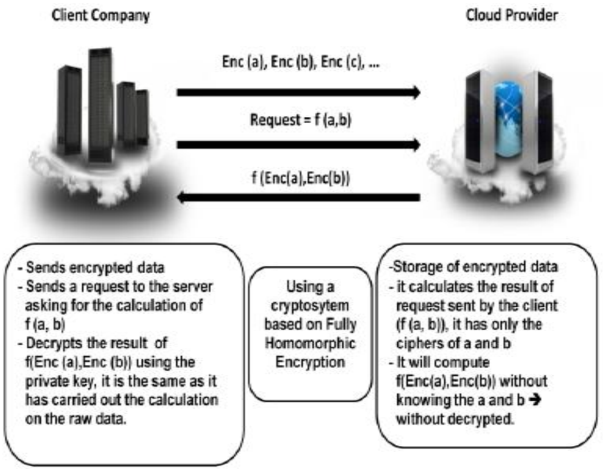

Client Company
Cloud Provider
Enc (a), Enc (b), Enc (c), ...
Request = f (a,b)
f (Enc(a),Enc(b))
- Sends encrypted data
- Sends a request to the server asking for the calculation of f (a, b)
- Decrypts the result of f(Enc (a),Enc (b)) using the private key, it is the same as it has carried out the calculation on the raw data.
Using a cryptosytem based on Fully Homomorphic Encryption
-Storage of encrypted data
- it calculates the result of request sent by the client (f (a, b)), it has only the ciphers of a and b
- It will compute f(Enc(a),Enc(b)) without knowing the a and b ➔ without decrypted.

Fig 1. Homomorphic encryption applied to the cloud computing

## 4. RSA CRYPTOSYSTEM

The RSA cryptosystem is the extensively used public-key Cryptosystem:

**Key Generation**: KeyGen(p, q)
**Input**: Two large primes – p, q
Compute n = p . q
φ (n) = (p - 1)(q - 1)
Choose e such that gcd(e, φ (n)) = 1
Determine d such that e . d ≡ 1 mod φ (n)
**Key:**
public key = (e, n)
private key= (d, n)
**Encryption:**
c = me mod n
where c is the cipher text and m is the plain text

RSA consist to increasing Homomorphic property i.e., it's doable to search out the merchandise of the plain text by multiplying the cipher texts. The results of the operation are the cipher text of the merchandise. Given ci = E(mi) = mie mod n, then (c1 . c2) mod n = (m1 . m2)e mod n Example:

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < φ(n) and e and n are co-prime. Let e = 7
- Compute a value for d such that e . d ≡ 1 mod φ (n). One solution is d = 3
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- Example of Homomorphic property: Now, let m1=2 and m2=3 c1 = m1e mod n=27 mod 33=29 c2 = m2e mod n=37 mod 33=9

c1.c2 = 29 * 9 = 261 By decrypting (c1.c2) we get: 2613 mod 33 = 6 = 2 * 3

## 5. SYSTEM ARCHITECTURE

Architecture can be implemented in 2 modules. 1. User 2.Admin

**User module**:

- ➢ Stores the data in to cloud, for this the user should be registered in the cloud server and has to be logged in and has to be search for particular index of image/data/ text. The search results will be returned by the cloud server if the key entered by the client is valid.

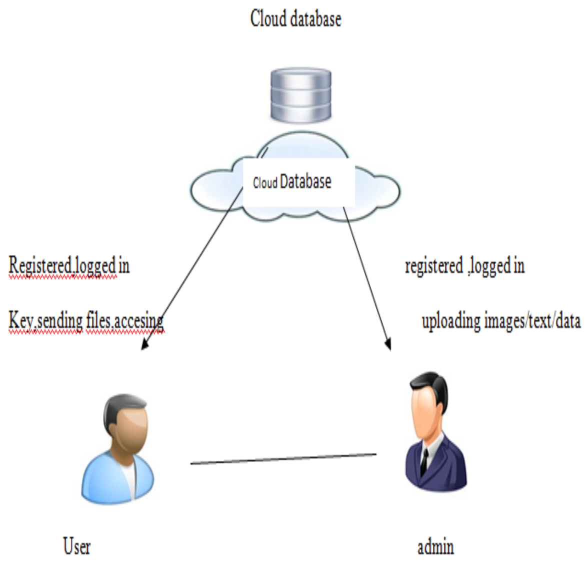


Fig 2: System Architecture

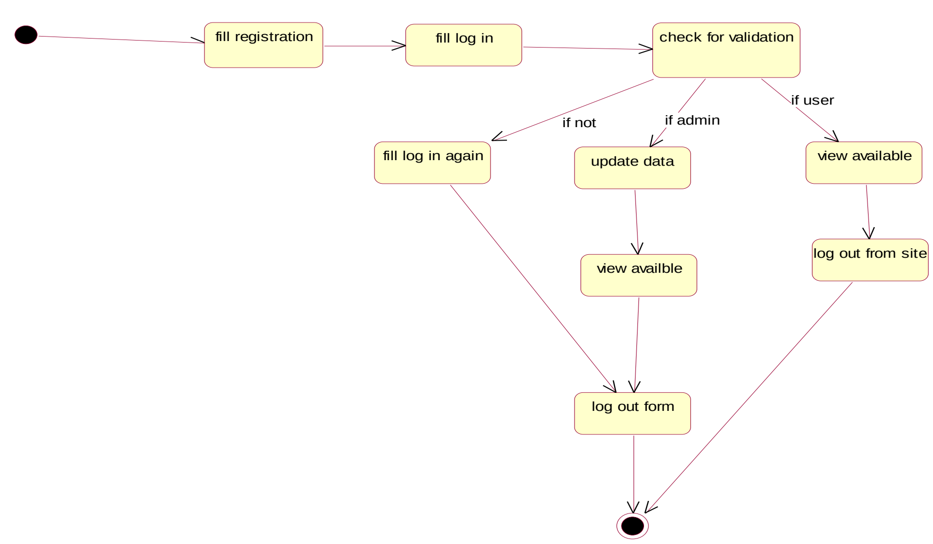


Fig3. System State Diagram

**Admin module:**

- ➢ The administrator has to be logged in; initially his duty is to store data i.e., uploading data, text, images. Cloud server process the admin stored data.

## 6. CONCLUSION:

Homomorphic secret writing is gaining increasing attention from varied views as cloud computing is turning into more and more widespread and dynamic the means individuals use IT technology to manage their information. Homomorphic secret writing one amongst the foremost appropriate secret writing algorithms for enabling information in cloud storage to be processed in its encrypted kind. The cloud computing security supported Homomorphic secret writing could be a new thought of security that permits providing results of calculations on encrypted information while not knowing the information on that the calculation was allotted, with respect of the information confidentiality. Homomorphic secret writing theme an extreme approach that gives information security that is a tremendous breakthrough in resolution a central open drawback in cryptography.

## REFERENCES:

[1]Vic (J.R.) Winkler, "Securing the Cloud, Cloud Computer Security, Techniques and Tactics", Elsevier, 2011.

[2] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In 18th Annual Eurocrypt Conference (EUROCRYPT'99), Prague, Czech Republic , volume 1592, 1999

[3] Julien Bringe and al. An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication, Springer-Verlag, 2007.

[4] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 21(2) :120-126, 1978. Computer Science, pages 223-238. Springer, 1999.

[5] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 469-472, 1985.

[6] Craig Gentry, A Fully Homomorphic Encryption Scheme, 2009.