IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Special Issue, 6, March 2019 E-ISSN: 2347-2693

A Survey on Securing Cloud Service Data by Using Homomorphic Encryption

J. Sai krishna[1*], S. Muni Kumar[2], K. Venkataramana[3]

[1]Dept. of Computer Applications, KMM Institute of PG Studies, Tirupati, India
[2]KMM Institute of PG Studies, Tirupati, India
[3]Dept. Of Computer Applications, KMM Institute of PG Studies, Tirupati, India

Corresponding Author: saikrishnaj2@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7si6.6672 | Available online at: www.ijcseonline.org

Abstract— In Recent trends shows Cloud computing technology is adopted by many IT companies as it reduces the investment burden for infrastructure, software, hardware or any reasonably resource in a company. However, one amongst the most important problems in implementing or adopting cloud is threats due to security breaches. To ensure security, countless ancient secret writing algorithms are used like various truthful cipher mechanisms, RSA, Homomorphic secret writing etc. however these algorithms are solely accustomed to convert plain text into cipher text during transit or at storage.Homomorphic encryption can be a particular type of encryption where mathematical operations on the cipher text is like mathematical operations on the corresponding plaintext. Homomorphic encryption (HE) is fascinating on account of the particular proven fact it can operate on big databases. In this paper discussed and studied the fundamental concepts of HE, along with various homomorphic encryption schemes andtheir possible implementation in cloud computing.

Keywords—*cloud computing,Homomorphic encryption, Security, Homomorphic Encryption in cloud computing*

I. INTRODUCTION

Cloud computing is one in all the foremost emerged net based Technology that garnered a good attention of researchers from tutorial and trade . Cloud computing provides on demand Services over Network(SoN) i.e,"Access services anytime from anyplace in pay-per-use fashion." a bent to any or all apprehend that the cloud or on-demand computing brings heaps of advantage to the computer science of those days and tomorrow. The adoption of cloud usage depends on security and protection that the cloud service produce ensure and also the manner a consumer can keep their personal information confidential Our basic construct was to encode the data before effort to the Cloud provider. But there is a haul still faced by the consumer. as a results of the Cloud provider should perform the calculations on data to retort the request from the consumer so he ought to provide the key to the server to rewrite the data before execute the calculations required, that might have an impression on the confidentiality of knowledge hold on inside the Cloud. how modify to perform the operations on encrypted data whereas not decrypted them is that the Homomorphic writing.

The Data transferred to the Cloud tend to use customary cryptography ways to secure this knowledge, when try to do the calculations on information placed on a far off server, it is necessary that the Cloud provider has access to the knowledge, so it will decipher them. throughout this paper tend to propose the applying of how to perform the operation on encrypted information whereas not decrypted and provide constant result likewise that the calculations were administrated on info whether or not or not you are running applications that share photos to a lot of mobile users or you're supporting the crucial operations of your business, a cloud services platform provides speedy access to versatile and low value IT resources. With cloud computing, you don't ought to build large direct investments in hardware and pay an excellent deal of it slow on the work of managing that hardware. Instead, you may provision exactly the proper kind and size of computing resources you would like to power your newest bright arrange or operate your IT department. you may access as many resources as you would like, nearly instantly, and only line up of what you utilize. Theory of Evolution.at the moment his student Rube Goldberg increased genetic rule within the year 1989. Genetic rule it's a tool to unravel numerous optimisation issues like whole number non linear issues. it's oft utilised for locating higher best answer for all combination of issues.

II. LITERATURE REVIEW

MahaTebba et al.inspected the core application eventualities of various Homomorphic coding cryptosystems eg: (RSA, Paillier, El Gamal, Gen-try etc.) on a Cloud Computing

environment[1]. Further, comparisionis being performed supported main four specialities ”Homomorphic coding type”, ”Privacy of data”, ”Security applied to” and”the keys used”. ReemAlattas et al. introduced the applying of pure mathematics Homomorphic coding mechanism, supported Fer-mat’s very little Theorem on cloud computing for higher security[2]. To fix the difficult drawback of knowledge privacy at the side of confidentiality within the cloud, totally HomomorphicEncryption(FHE) mechanism is Associate in Nursing explication, wherever the encrypted data is handled[3],and it returns the leads to encrypted manner. In spite of, totally homomorphic coding mechanism runs in relatively slower mode thence, the quicker totally homomorphic coding mechanisms square measure considerably required. Gentry’s projected coding mechanism is totally homomorphic however having impediment of slower performance.Lot of varied mechanisms are recommended in recent years to remarkably speed up the performance action of totally homomorphic coding schemes.

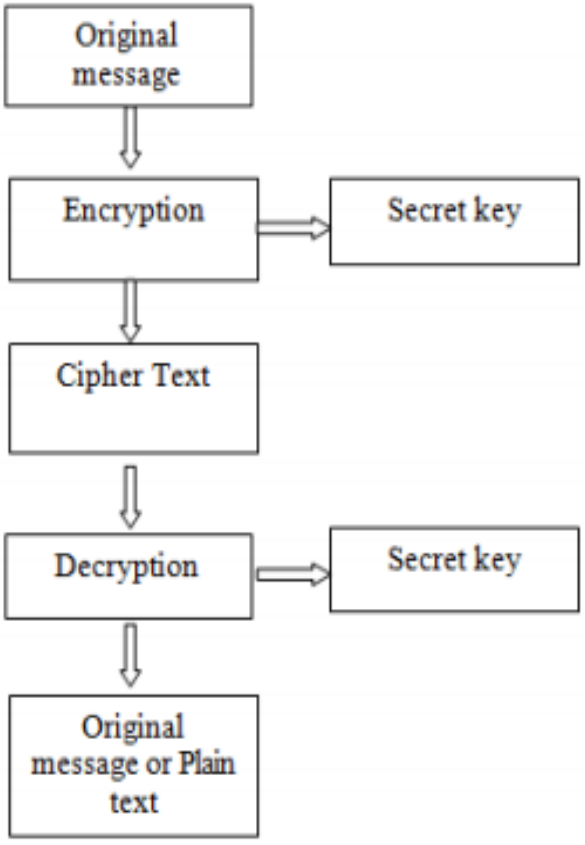

Figure 1-Symmetric Key Cryptogray

In fig. 1, Symmetric key Cryptography is shown. Here for encryption, plain text is converted into cipher text, with use of secret key. And at decryption time it using again same secret key to convert cipher text into plain text

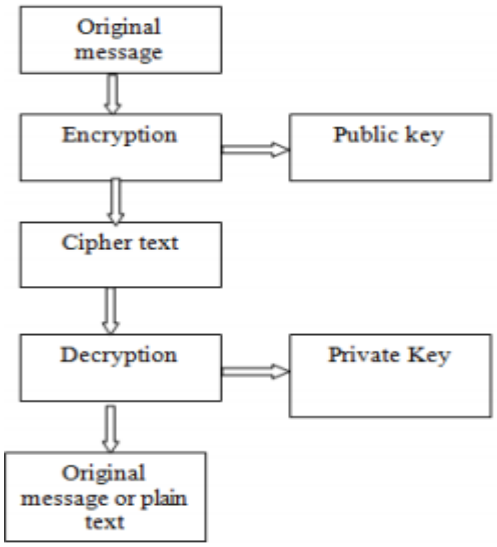

Figure 2-Asymmetric Key Cryptography

In fig. 2, uneven key Cryptography is shown. Here for secret writing method, plain text is regenerate into cipher text, with use of public key. And at cryptography time it victimisation non-public key to convert cipher text into plain text.

`Asymmetric key cryptography is employed two completely different keys: a public key and a personal key for secret writing and cryptography severally. non-public secret is can not be derived from public key. This theme, offer abundant strength of security[4].

III PROPOSED METHODOLOGY

A. Cloud Computing

1). What is Cloud Computing?

Cloud Computing typically named as “the cloud”, in straightforward terms means that storing or accessing your information and programs over the net instead of your own disk drive.

Everything today is enraptured to the cloud, running within the cloud, accessed from the cloud or is also hold on within the cloud.

2). *Where exactly is this cloud?*

So to answer this question during this what's cloud computing diary, it's somewhere at the opposite finish of your web affiliation wherever you store your files and may be accessed from anyplace within the world. this might be an enormous deal for you, primarily owing to 3 reasons:

You do not have to be compelled to maintain or administer any infrastructure for identical.

It will ne'er run out of capability, since it's nearly infinite.

You can access your cloud primarily based applications from anyplace, you only want a tool which might connect with the net.

3).Cloud Computing Architecture:
Cloud ADPS is split into 2 sections: the side and therefore the backside. side through that user will act with the server and backend is that the server that provides information to the consumer. Between server and consumer network is functioning as middleware.

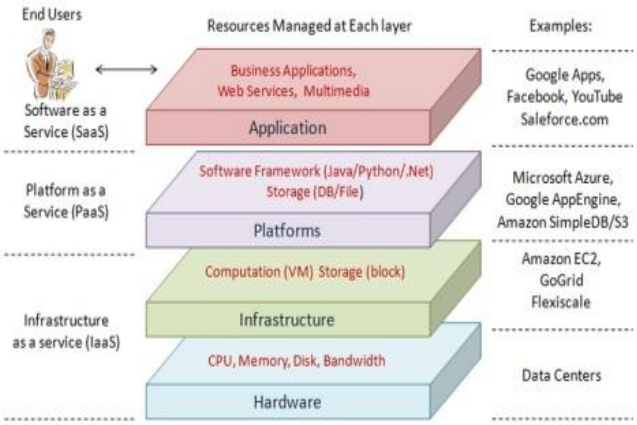

Figure 3-

Cloud Computing Architecture

4). Security issues in cloud computing
Pointed out some security challenges in cloud computing, which are as below:-
When customers square measure outsourcing/transfering their personal information to any third party, then there's abundant responsibility of each security and compliance. Therefore, it's necessary that customers ought to totally religion in their cloud service supplier Cloud computing consists of many technologies example: databases,network structure, operative systems, virtualization state of affairs, re-sources and processes planning, dealing management, load equalisation issue, memory management etc. So, because of use ofthese large choice of technologies, atiny low security weakness in anyone of those technologies might knock down the whole system

B.Encryption of Cloud Data
Organizations seeking to guard sensitive and mission-critical knowledge quickly notice that there's no single answer to stay all systems utterly secure.Online knowledge security could be a advanced, quickly evolving landscape, requiring strong and stratified protections. secret writing is one tool in an exceedingly comprehensive defense-in-depth strategy to mitigate the chance of accidental and intentional knowledge breaches.Like each alternative technology tool, implementation should work at intervals a broader digital system, while not disrupting the aim that the system was designed to satisfy. Evaluating the advantages of secret writing against potential tradeoffs like value, performance, and in progress maintenance is at the guts of crucial the foremost effective and economical suggests that of mistreatment secret writing.

1).What is encryption?
Encryption takes plaintext (your data) and encodes it into illegible, disorganized text mistreatment mathematical algorithms, effectively rendering information illegible unless a science secret's applied to convert it. coding ensures information security and integrity, albeit accessed by Associate in Nursing unauthorized user, provided the coding keys haven't been compromised. coding will defend information in motion, stated coding in transit or coding on the wing, further as at rest; which means in storage. coding usually happens at multiple levels of a system, acceptable to the context of use and alternative system element

2).Cloud encryption challenges

One of the first challenges related to encoding as a full is that the straightforward undeniable fact that it's underutilized, despite its tried effectiveness at bolstering information security. As a lot of enterprises and SMBs demand bigger security measures from cloud suppliers to boost compliance whereas maintaining potency, use is changing into a lot of widespread.

Encryption drives prices for cloud storage suppliers (and ultimately their customers) because of the extra information measure needed to write information before it's transferred to the cloud. As a result, several suppliers limit their cloud encoding services whereas some cloud storage customers merely write their own information on-premises before it's stirred to the cloud. Some cloud customers can opt for this approach regardless, because it will save prices whereas keeping the complete encoding method and every one keys among their surroundings, transferring information to the cloud solely once it's been encrypted.

3).Benefits of cloud encryption
The key advantage of cloud cryptography is that the same as in any application of encryption: encrypted information is merely legible for licensed parties with access to the decipherment keys. Encrypting information ensures that although that information falls into the incorrect hands, it's useless as long as its keys stay secure. this is often particularly useful once information is being hold on within the cloud, because it protects information contents within the event that a supplier, account, or system is compromised.Cloud cryptography is additionally vital for industries that require to fulfil restrictive compliance needs. Encryption, once combined with alternative security measures, permits enterprises to fulfil the tight compliance needs of HIPAA (for attention organizations and business associates), PCI DSS (for e-commerce and retail organizations), and SOX (for money reporting).Any

organization at intervals these industries that has adopted the cloud should be ready to fulfil the safety challenges that go together with mistreatment cloud storage and services. Cloud cryptography permits firms to be proactive in their defence against information breaches and cyberattacks and has become a necessity in today's data-driven world.

C. TECHNIQUES IN HOMOMORPHIC

first made by Craig upper crust in 2009. Homomorphic coding differs from typical coding strategies therein it permits computation to be performed directly on encrypted information while not requiring access to a secret key. The results of such a computation remains in encrypted kind, and might at a later purpose be discovered by the owner of the key.

HOMOMORPHIC ENCRYPTION

1).History of the Homomorphic encryption

In 1978 Ronald Rivest, Elmore John Leonard Adleman and Michael Dertouzos advised for the primary time the construct of Homomorphiccryptography . Since then, very little progress has been created for thirty years. The cryptography system of ShafiGoldwasser and Silvio Micali was planned in 1982 was a demonstrable security cryptography theme that reached an interesting level of safety, it had been associate additive Homomorphic cryptography, however it will code solely one bit. within the same construct in 1999 Pascal Paillier was conjointly planned a demonstrable security cryptography system that was conjointly associate additive Homomorphic cryptography. Few years later, in 2005, Dan Boneh, Eu-Jin Goh and KobiNissim fictional a system of demonstrable security cryptography, with that we will perform a vast range of additives however only 1 multiplication.

2).What is HomomorphicEncryption in Cloud computing

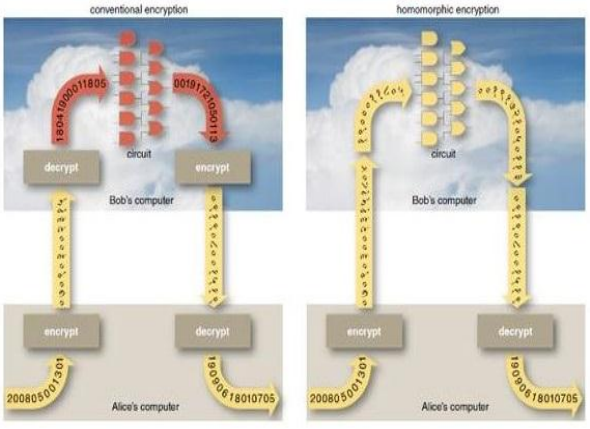

Figure :4

Homomorphic cryptography systems square measure wont to perform operations on encrypted information while not knowing the key (without decrypted), the shopper is that the solely individual of the key. after we rewrite the results of the operation, it's a similar as if we have a tendency to had distributed the calculation on the information.

The difference between the conventional encryption schemes and homomrphic encryption in cloud

An cryptography is homomorphic, if: from Enc (a) and Enc(b) it's doable to cypher Enc (f (a, b)), wherever f will be: +, ×, and while not victimisation the non-public key . Among the Homomorphic cryptography we have a tendency to distinguished in step with their operation to assess on information. The additive Homomorphic cryptography (addition of the raw data) is that the Pailler and Goldwasser-Micalli cryptosystems and therefore the increasing Homomorphic cryptography (only merchandise on raw data) is that the RSA and El Gamal cryptosystems

Encryption is that the science or art of remodeling plain text messages to AN "encrypted" kind hidden ,homomorphic cryptography could be a type of cryptography within which the formula we have a tendency to explicit higher than is correct in alternative words the "f" is AN cryptography algorithmic program and therefore the cryptography of the merchandise of 2 numbers is adequate to the merchandise of the encryptions of the numbers :E(a.b) = E(a).E(b)

E is an encryption algorithm or in more proprietary terms a scheme .

D.PARTIALLY HOMOMORPHIC ENCRYPTION SCHEMES

In this section, the survey of assorted homomorphic secret writing themes like pure mathematics homomorphic secret writing scheme supported updated ElGamal (AHEE), Non-interactive exponential homomorphic secret writing algorithmic program (NEHE), homomorphic Cryptosystem (EHC), Brakerski-Gentry-Vaikuntanathan (BGV) etc is completed here.

1).Paillier

The Paillierthеme , was fictional by Pascal Paillier in 1999 it's a probabilistic theme that's homomorphic with relevance addition (the add of 2 ciphertext is capable the ciphertext of the add of the 2 plaintext equivalents) and to multiplication by a relentless . Paillier could be a form of keypair-based cryptography. this suggests every user gets a public and a personal key, and messages encrypted with their public key will solely be decrypted with their personal key.

Suppose E is that the paillier secret writing perform then we've the subsequent 2 properties :

E(a)+E(b) = E(a+b)

E(a)^b = E(a * b)

Paillier consists of 3 algorithms actually 3 algorithms area unit necessary to form associate secret writing theme .

First you would like a Key generation algorithmic rule, second associate secret writing algorithmic rule and last a decipherment algorithmic rule let's see however Paillier implement those .

Key Generation

To generate a key you decide on 2 giant primes p and Q specified :

gcd(pq,(p-1)(q-1)) = one In otherwords the merchandise of p and Q and (p-1) and (q-1) area unit comparatively prime (their greatest common factor is 1) .

Then you reckon 2 parameters n & lambda specified : * n = pq and lambda = lcm(p-1,q-1) lowest common multiple is that the least integer for instance lcm(4.8) = 16

Select a random number g like g belongs to the set of integers modulo n square .during this case (p and Q area unit primes of an equivalent length) you'll choose g as n+1

Compute alphabetic character like alphabetic character = lambda^-1 mod n (modular increasing inverse)

The public key's (n,g) and therefore the personal key's (lambda,mu)

Encryption

suppose m is your message and r a random number such as :

m < n and r < n

c = g^m * r^n mod n^2

c is the ciphertext of m

Decryption

m = L(c^lambda mod n^2) * mu mod n

L(x) = (x-1) / n

Example with small parameters and proof of homomorphism

let p = 11 and q = 13

n = pq = 143

g = n+1 = 144

The public key is (143,144)

Let's encrypt the answer of the universe and send it to the Zorbs(habitants of Zorbis planet)

m = 50

we pick r : r = 23

c = g^m * r^n (mod n^2)

= 144^50 * 23^143 (mod 143^2) = 9637

m = L(c^lambda mod n^2) * mu mod n

lambda = (p-1)*(q-1) = 10*12 = 120 mu = lambda^-1 mod n = 120^-1 mod 143

m = L(9637^120 mod 143^2) * (120^-1 mod 143) mod 143

m = 50

note that you should use modular inverse to compute mu

Homomorphic Properties

Now that we have a tendency to outlined the the procedure to get a keypair, code and decode let's discuss the homomorphic properties of Paillier .

Addition :

The product of 2 ciphertexts decrypts to their total , if i need to try and do addition on ciphertexts comparatively to my plaintexts I even have to calculate the merchandise of the ciphers

Proof suppose E is that the encoding formula and money supply and money supply the plaintexts : E(m1) * E(m2) = (g^m1*r1^n)(g^m2*r2^n) mod n^2 = g^(m1+m2) (r1r2)^n mod n^2 = E(m1+m2)

Multiplication:

If I even have a plaintext m and a continuing k then the encoding of their product evaluates to the cipher of m raised to the facility k .

Proof same suppositions regarding E,m1,m2 as before : E(m1)^m2 = (g^m1+r1^n)^m2 mod n^2 = g^(m1m2) (r1^m2)^n mod n^2 = E(m1m2)

2).BGV Encryption Scheme

Dealing with whole number vectors (whose security depends on the hardness of decisional LWE (Learning with Errors) and handling the whole number polynomials (whose security depends on the hardness of the decisional R-LWE (Ring LWE) area unit 2 versions of the cryptosystem. BGV is associate degree uneven coding theme which might be used for the coding of the bits.

Encrypt(Plaintext *m*, PublicKey *Pub*): Ciphertext *c*
Decrypt(Ciphertext *c*, PrivateKey *Priv*): Plaintext *m*
Level shifting operations   **Rescale**(Cipertext *c*): Ciphertext *c'*   **SwitchKey**(Augmented Cipertext *c*): Ciphertext *c'*
Homomorphic operations   **Add**(Ciphertext *c*1, Ciphertext *c*2): Ciphertext *csum*   **Mul**(Ciphertext *c*1, Ciphertext *c*2): Ciphertext *cmul*

Fig. 5

3*). Gorti's Enhanced Homomorphic Cryptosystem (EHC)*

EHC is that the new increased Homomorphic Cryptosystem used for homomorphic cryptography / decoding with IND-CCA secure. There square measure varied applications of this kind of homomorphic cryptography within the real time. Homomorphic cryptography has the fundamental thought that the pc can perform the computations on the already encrypted information while not having any data of its real worth. And finally this computed encrypted message or information are going to be sent back as a result and decrypted. This decrypted result should be adequate the meant computed worth if performed on the important information.

Chose large prime number ' p ' and another prime number ' q '
Calculate m = p * q
Generate a random number ' r '.
r,q and m Kept secret. Secret values r,q and m

Shared key : p

Encryption
Encrypt(X,m,p,q,r)
Assume X ∈ *Zp*
Compute $Y = (X + r*pq) \pmod m$
Output Y ∈ *Zc*

Decryption
Decrypt(Y,p)
input Y ∈ *Zc*
compute X = Y mod p output X ∈ *Zp*

Fig. 6

4) .Algebra Homomorphic Encryption Scheme Based On Updated ElGamal (AHEE)

This is the changed sort of the digital signature normal DSS given by the authority in America[27]. Te security of the AHEE is IND-CPA that is that the highest level of the protection of AHEE. Additive similarity of this rule refers a similar k for secret writing however uses the random variety of k in E1() that makes AHEE able to resist plaintext attack. The AHEE is that the set of the totally similarity. AHEE has been well-tried to be secure. This description of totally similarity is advanced by Rivest, Adlemanand Dertouzos is as follows .power tool and Tschudin outlined additive and increasing homomorphism's on whole number Ring(Homomorphic secret writing theme, particularly HES)Homomorphic operations:

Step 1: select any two prime numbers say p and q

Step 2: calculate the product of those two prime numbers. Say N = p * q. where p and q being confidential and N is public.

Step 3: select random number x and a root g of GF(p). where g and x are smaller than p.

Step 4: calculate $y = g^x \bmod p$. use this y for the encryption.

Step 5: encryption will be performed in following two steps:

1. Select random integer number r and apply following homomorphic encryption.
   $E_1(M) = (M+r*p) \bmod N$.
2. Select random integer number k, and the encryption algorithms are:
   $E_g(M) = (a,b) = (g^k \bmod p, y^k E_1(M) \bmod p)$

Step 6: Decrypted algorithm D_g () is $M=b\times (a^x)^{-1} \pmod p$.

Fig. 7

5) .Fully Homomorphic Encryption Scheme (FHE): -

This is the second stage of the cryptography method. This cryptography theme is predicated on Criag. the flexibility to question, index and work on encrypted information while not decrypting it makes this cryptography technique distinctive. This theme performs 2 operations, additive and increasing homomorphic. we'll be mistreatment solely additive algorithms. At this stage, we've ciphertext from the primary cryptography and therefore the non-public key used. This Ciphertext and personal key can currently be encrypted along by mistreatment additive homomorphic cryptography.

FHE is taken into account as way more powerful and a good way to secure the outsourced information in associate degree efficient manner.Gentry's planned theme has 3 significant components:-

(1) A somewhat homomorphic cryptography scheme(SWHES)

(2) A bootstrappable cryptography scheme(BES)

(3) a mixture of higher than 2 part

Additive homomorphic formula supported C aristocracy is that the following this is often the bases: - Enc (a + b) = Enc (a) +Enc (b) wherever c = cipher text m = message (Plaintext) Q = range} p = positive odd variety r = random number c =m+2r+pq to induce m m = (cmod p) mod2 Not p and Q < 2r + m, (cmod p) mod2 = (2r + m) mod 2= m From the additive bases Enc (a + b) = Enc (a) +Enc (b) Enc cl c2 cl = gml. rln mod n two c2 = gm2. r2n mod n two Enc(c one + C 2) = Enc (c one) + Enc (c 2) Enc(c 1 + C 2) = gml. rln mod n two + gm2. r2n mod n two Enc(c one + C two) = gml+m2 (rlr2)n mod n 2

IV. SCHEME AND IMPLEMENTATION

For every kind of calculation on the information hold on within the cloud, tendency to should choose the totally Homomorphic cryptography that is capable to execute every kind of operations on encrypted knowledge while not decrypted it. In 2009 Craig upper crust of IBM has planned the primary cryptography system "fully homomorphic" that evaluates AN discretional range of additives and multiplications and so calculate any kind of operate on encrypted knowledge .the applying of totally Homomorphic cryptography is a vital wall in Cloud Computing security; additional usually, we have a tendency to may source the calculations on confidential knowledge to the Cloud server, keeping the key which will decode the results of calculation. In our implementation, we have a tendency to analyze the performance of existing Homomorphic cryptography cryptosystems, a tendency to square measure functioning on

a virtual platform with ESX as a Cloud server, a VPN network that links the Cloud with the client (enterprise), then when tendency to started by simulating completely different eventualities victimisation the pc pure mathematics System stone tools , focusing on:

Security of cloud computing supported absolutely Homomorphic coding may be a new conception of security that is change to produce the results of calculations on encrypted information while not knowing the raw entries on that the calculation was dispensed respecting the confidentiality of information. Our work is predicated on the appliance of absolutely Homomorphic coding to the safety of Cloud Computing: a) Analyze and improve the present cryptosystem to permit servers to perform numerous operations requested by the shopper. b) Improve the complexness of the Homomorphic coding algorithms and study the interval to requests in keeping with the length of the general public key.

V. CONCLUSION

In this paper is used to provide homomorphic secret writing technique which is in security on cloud. Homomorphic secret writing may be a new thought of security that allows providing results of calculations on encrypted knowledge while not knowing the data on that the calculation was meted out, with respect of the information confidentiality. during this paper I actually have projected Paillier algorithmic program for homomorphic secret writing victimisation proxyRe-encryption algorithmic program that forestalls cipher knowledge from Chosen Cipher text Attack (CCA).So this method is safer than existing system. In future will work efficiently of the system by reducing size of the key and that we may also check proxy Re-Encryption technique for alternative Homomorphic secret writing theme. Security of cloud computing supported Homomorphic secret writing may be a new thought of security that is change to produce the results of calculations on encrypted knowledge while not knowing the raw entries on that the calculation was meted out respecting the confidentiality of knowledge. Our work relies on the applying of Homomorphic secret writing to the protection of Cloud Computing

REFERENCES

[1]. Ms. Parin V. Patel, Mr. Hitesh D. Patel, Prof. Pinal J. Patel, "A Secure Cloud using Homomorphic Encryption Scheme", International Journal of Computer Science Research & Technology (IJCSRT) Vol. 1 Issue 1, June-2013.

[2].Maha TEBAA* ; Said EL HAJJI** University Mohammed V – Agdal, Faculty of Scienc "Homomorphic Encryption method applied to Cloud Computing" Abdellatif EL GHAZI Laboratory of Research – Institute of Vinci Rabat

[3].kamalkumarchauhan,Amit K.S Sanger ,Ajaiverma" Homomorphic encryption for data security in cloud computing".

[4].PG Student, Maharashtra Institute Of Technology(MIT), Pune Maharashtra Institute Of Technology(MIT) Iram Ahmad 1 and ArchanaKhandekar" Homomorphic Encryption Method Applied to Cloud Computing"

Authors Profile

Mr J Saikrishna has completed UG in S.V.University in 2016 and currently pursuing Master of Computer Applications from *KMM Institute of PG Studies, S.V university, Tirupati, India.*

Dr.K. Venkataramana received his P.hd in Computer Science from S.V.University and currently working as a Associate Professor in Dept of Computer Science and Applications in KMM Inst. Of P.G Studies(Recognized by AICTE). He has work experience of 20 years in Teaching and published his research work in about 30 papers in reputed journals.

