Secure Email Service in Cloud by using Modified Homomorphic Encryption Algorithm

J. Sai Krishna[1] Dr. K. Venkataramana[2]
[1]Student [2]Professor
[1,2]Department of Computer Applications
[1,2]KMM Institute of PG Studies, Tirupati, India

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 and their possible implementation in cloud computing.

Key words: Homomorphic Encryption Algorithm, Services over Network (SoN), 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[2]. introduced the applying of pure mathematics Homomorphic coding mechanism, supported Fer-mat's very little Theorem on cloud computing for higher security[3]. To fix the difficult drawback of knowledge privacy at the side of confidentiality within the cloud, totally Homomorphic Encryption(FHE) mechanism is Associate in Nursing explication, wherever the encrypted data is handled[4],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.

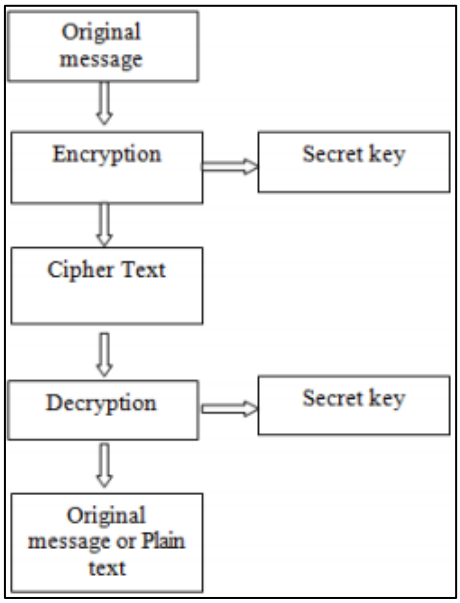

Fig. 1: Symmetric Key Cryptogray

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

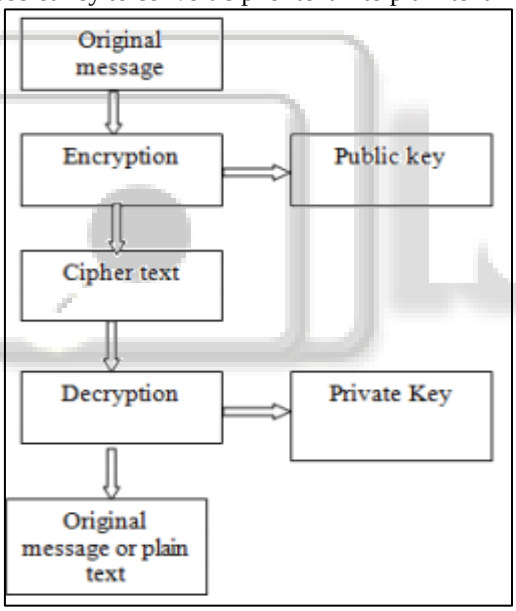

Fig. 2: Asymmetric Key Cryptography

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 cannot be derived from public key. This theme, offer abundant strength of security[4].

A. 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.

B. 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.

C. Cloud Computing Architecture:

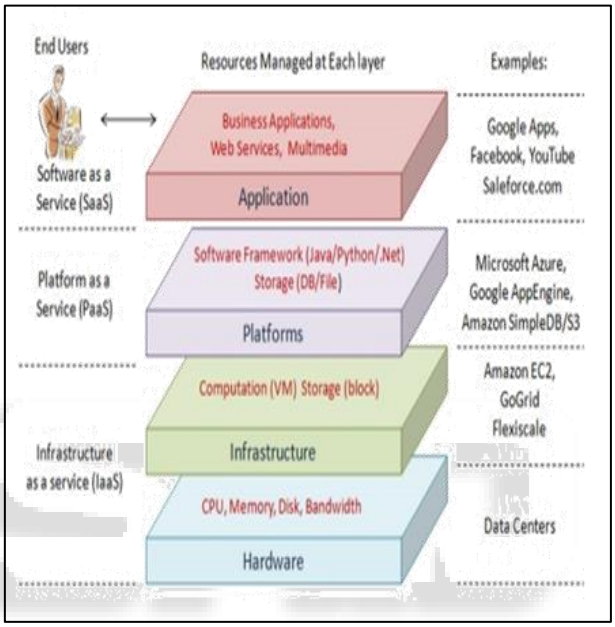

Fig. 3: Cloud Computing Architecture

D. Security issues in cloud computing

Pointed out some security challenges in cloud computing, which are as below:-

When customers square measure outsourcing/transferring 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 of these large choice of technologies, a tiny low security weakness in anyone of those technologies might knock down the whole system

III. PROPOSED METHODOLOGY

A. Homomorphic Encryption

1) What is Homomorphic Encryption in Cloud computing

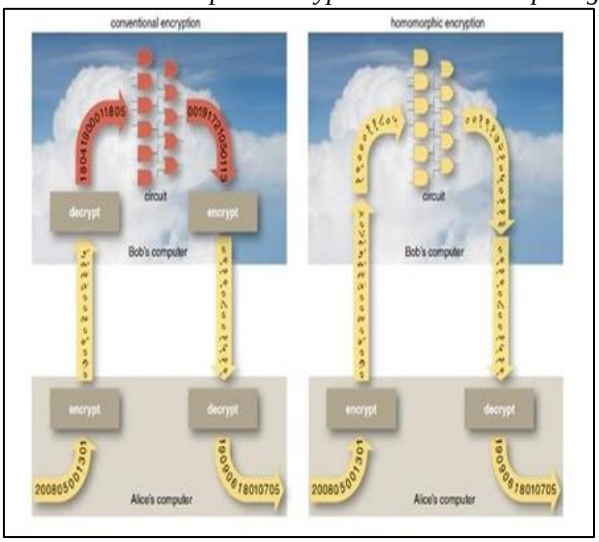

Fig. 4:

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.

B. Partially Homomorphic Encryption Schemes

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 .based on pailier homomorphic encryption algorithm. I am developed this modified algorithm.

IV. PROPOSED ALGORITHM

A. Modified Homomorphic Encryption Scheme

1) Key Generation:

1) Generate prime number using seieve of erathosthese(let P and Q)
   1.1.for all number m=1,2,….n if m is unmarked
   1.2.add m to prime list
   1.3. mark all its multiple ,lesser or equal
   Than n(k*m<=n,k<=2);
   1.4. otherwise if m is marked then it is a composite number
2) p and q values from m.
3) find GCD(pq, (p-1)(q-1))=1
   3.1. using euclidian algorithm
   3.2 .if p<q exchange p and q
   3.3. Divide a by q and get remainder r if r=0
   Rebort q a\as the GCD
   3.4. replace p and q and replace b by r
4) n=pq and lambda =lcm(p-1)(q-1)
5) g is n+1
6) mu=lambda^-1mod n
   Now

Public key(n,q)(22/7
Private key(lambda,mu)*22/7

2) Encryption

1) let m is message and r is a random number m<n and r<n
2) c=g^m*r^n mod n^2

3) Decryption

1) m=l(c^lambda modn^2)*mu mod n

V. RESULT AND ANALYSIS

Here using Modified Homomorphic encryption algorithm we can give security for cloud mail service, we can use these algorithm for office software sans cloud based softwares. 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.

A. Registration

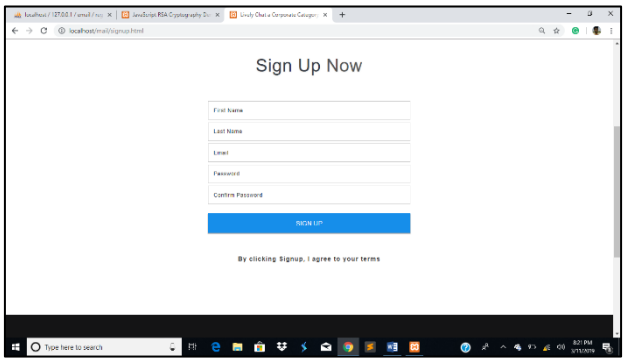

Fig. 5:

B. Login

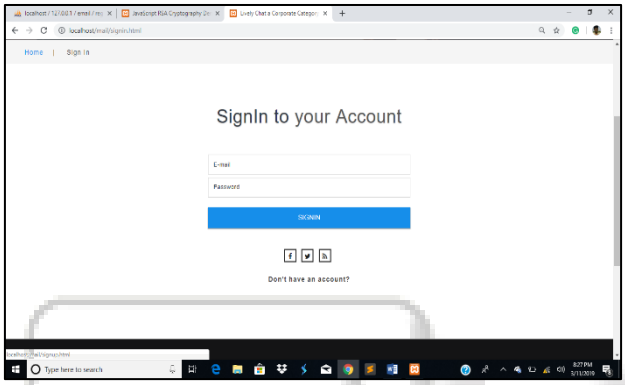

Fig. 6:

C. After Login He Need to Generate Public Key and Private Key Through That We Will Get Secret Key

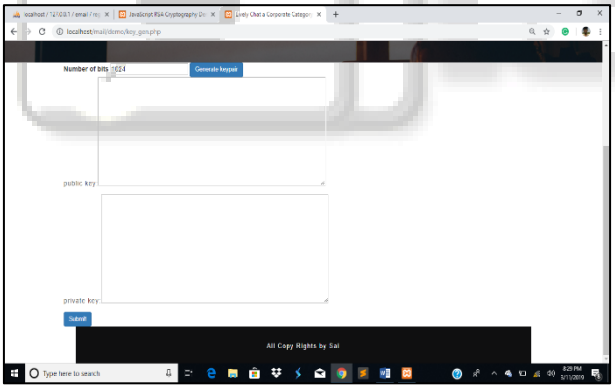

Fig. 7:

D. We Need Save This Secret Key Forther Reference

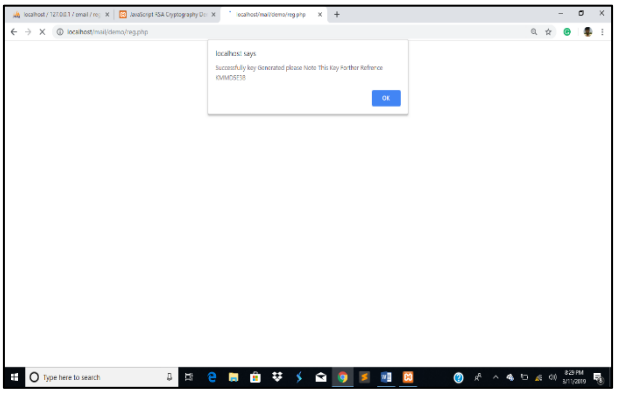

Fig. 8:

E. Write Message Before Enter Key

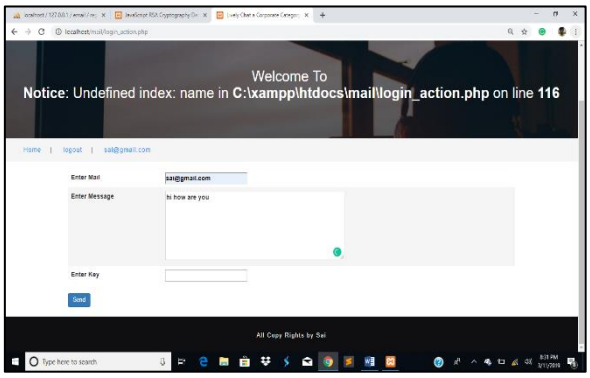

Fig. 9:

F. After Enter Key Data Will Be Encrypted

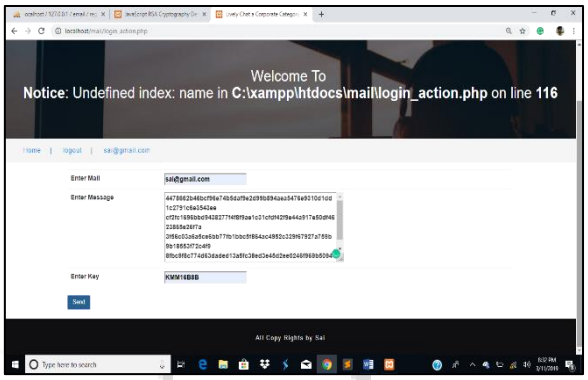

Fig. 10:

G. Now We Need To See the Original Data for That Login to Another Account

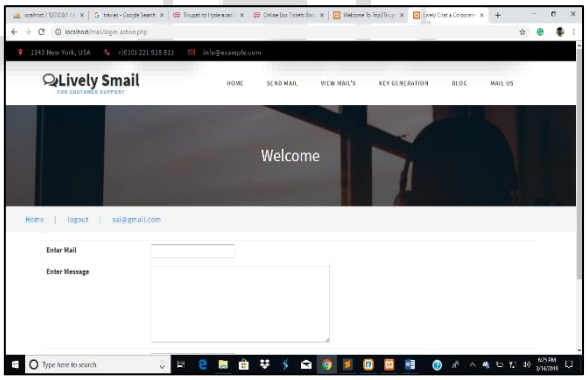

Fig. 11:

H. Click View Mail Option, We Got Sender and Encryption Data Which is Give by the Database.

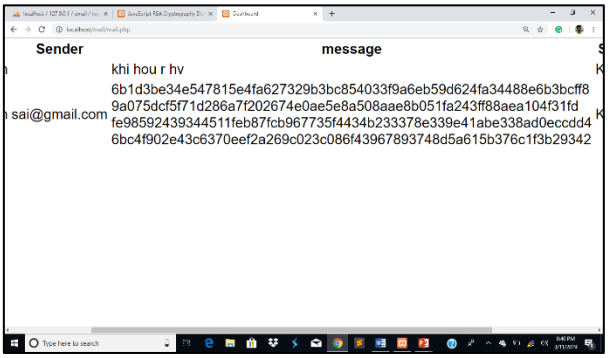

Fig. 12:

I. If We Want To View the Original Data We Need To Enter the Secret Key

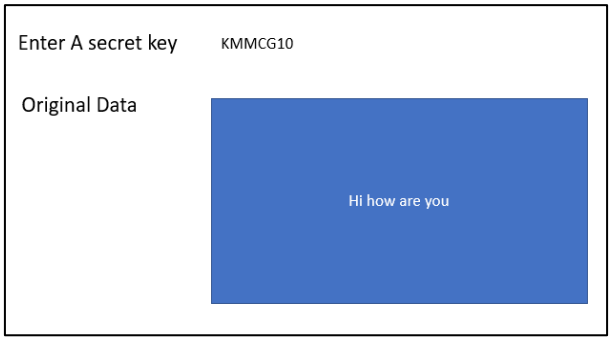

Fig. 13:

VI. 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 proxy Re-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. 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] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. ACM Transactions on Computation Theory, 6(3):13, 2014.
[2] Z. Brakerski and V. Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. SIAM J. Comput., 43(2):831–871, 2014.
[3] Pascal Paillier, "Public-key cryptosystems based on composite degree residuosity classes", In 18th Annual Eurocrypt Conference (EUROCRYPT'99), Prague, Czech Republic, volume 1592, 1999
[4] Vic (J.R.) Winkler, "Securing the Cloud, Cloud Computer Security, Techniques and Tactics", Elsevier, 2011.
[5] D. Boneh and al. Public key encryption with keyword search, proceedings of Eurocrypt 2004, LNCS 3027, pp. 506-522, 2004.
[6] E-Voting Simulator based on the Paillier Cryptosystem, Andreas Steffen, HSR Hochschule für Technik Rapperswil .
[7] Public-key cryptosystems based on composite degree residuosity classes (1999), Pascal Paillier

