Secure The Data using Modified Homomorphic Encryption and Paillier's Technique

R. Niranjan[1] Dr. K Venkataramana[2]
[1]Student [2]Assistant Professor
[1,2]Department of Computer Applications
[1,2]KMM Institute of PG Studies, Tirupati, India

Abstract— Homomorphic Encryption is a Scheme which performs the operations on encrypted data. A homomorphic encryption scheme allows evaluating of encrypted data even without knowing the secret decryption key. It can be applied on various system by using different public key algorithms. The major advantage of the Homomorphic encryption can be taken by cloud computing applications. It supports the algebraic operations to be computed on the encrypted data. In this paper, the focus of homomorphic encryption scheme is based on the prime integers. This paper includes additive and multiplicative Homomorphism. Homomorphic encryption has wide range of applications like secured electronic voting system. The paper mainly focus on enhanced homomorphic encryption using paillier cryptography.

Keywords: Homomorphic Encryption, Security, Paillie's Technique

I. INTRODUCTION

With the evaluation of communication networks and digital communication, secure communication and data security is of paramount importance. Today one way to reach secure communication is by the use of cryptography. When the data is to explored to the remote cloud server and the privacy of the sensitive data possible to attacks like un-trusted third party authentication computations, side channel attackes and implementation bugs in the system. Due to these attacks the homomorphic encryption is required to encrypt the computational data on server side. Thus a new idea of cryptosystem was proposed that allows the direct computation on the encrypted data. This concept is called "privacy homomorphism".

Then the concept of the privacy homomorphism[1] (homomorphic encryption) is introduced by the Rivest, Adleman and Dertouzos, which supports the computations on the encrypted data. While exclusively manipulating encrypted data, implicit additions multiplications on plaintext values can be performed by using the homomorphic encryption.

A. Homomorphism

Homomorphism is a algebraic term which refers mapping between the two groups (G,□) and (H,□). Let (G,□) and (H,□) are two groups over some algebraic operation. A function f:G➔H is called homomorphism.

B. Homomorphic Encryption

In 1978 Ronald Rivest, Elmore John Leonard Adleman and Michael Dertouzos advised for the primary time the construct of Homomorphic cryptography. Since then, very little progress has been created for thirty years. The cryptography system of Shafi Goldwasser 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 Kobi Nissim fictional a system of demonstrable security cryptography, with that we will perform a vast range of additives however only 1 multiplication.

Hmomomarphic encryption is the encryption is already encrypted data rather than on the original data with providing result as it is done on the plain text. The critical mathematical operations can be performed on the cipher text without changing the nature of the encryption.

C. Functions of Homomorphic Encryption

Homomorphic encryption is a set four functions as given below.

H={key Genaration, Encryption, Ealuation, Decryption}

1) Key Genaration: client will generate pair of keys publickey pk and secret key sk for encryption of plaintext in this encryption.
2) Encryption: Using secret key sk client encrypt theplain text PT and generate Esk(PT) and along with public key pk this cipher text CT will be sent to the server.
3) Evaluation: A Server has a function f for doing evaluation of cipher text 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. The fallowing Diagram shows the Encryption and Decryption process.

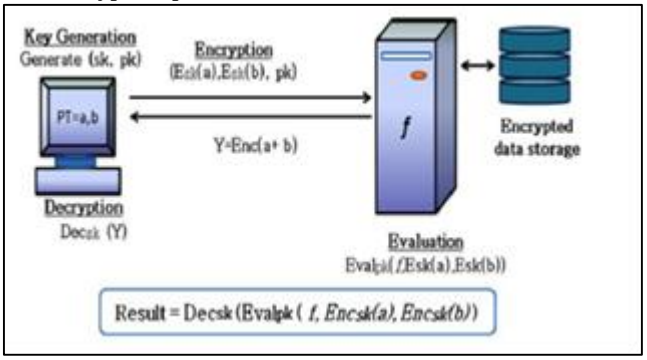


Fig. 1: Text Encryption and Decryption Process

D. Homomorphic Properties

The homomrphic encryption has two properties as stated below.

As the encryption functions is additively homomorphic, the following identities can be defined:

1) Homomorphic Addition of Plain Texts:
The product of 2 cipher texts will decrypt to the sum of their relative plaintexts.D (E (m1, r1) · E (m2, r2) mod n2) = m1 + m2 mod n.
2) Homomorphic Multiplication of Plain Texts:
The product of a cipher text with a plaintext raising will decrypt the sum of the related plaintexts, D (E (m1, r1) · gm2 mod n2) = m1 + m2 mod n.

II. RELATED WORK

Payal V. Parmar[1] Security is the prime demand as a result of cybercrimes are increasing today. Today, the public setting is required to be secure for protective the protection of information. There are several personal environments are- offered however to store the information over those environments maybe valuable than public space. Hence, most are convenient to store the information on public cloud i.e. Internet. There are several encoding algorithms are offered [6].Using those, the secure setting is created.

[6].Using those, the secure setting is created. Homomorphic encoding allows that secure setting within which the operations will be done on the already encrypted information and therefore the same result may be obtained as on original information [7]. There are several homomorphic encoding schemes are delineate during this paper that makes use of this approach. Lets take an example of computation delogation where the user doesn't have the required resources to perform the computation on the data. In this artice the user outsource his/her data to some service provider over the network or to the cloud. Now the user follows the following operation to perform the computation on his/her data. Pramod Kumar Siddharth[2] suggested the homomorphic properties of the cryptographic techniques take the attention of the scholars and makes it open research problem. The previous encryption schemes don't support the operations to be computed on the encrypted data, which may compromise the privacy of the sensitive data. The homomorphic encryption supports the mathmatical operations to be computed on the encrypted data. This algebraic property of the homomorphic encryption scheme have a wide application areas such as secure electronic voting, multiparty computation, private searching, delegation of computation and many more. In this article we proposed a homomorphic encryption scheme based on the Carmichael's theorem over integers. The operations in the operations are modular arithmetic. The paper also discuss the security scheme and further optimization are pointed out.

Tannishk Sharma [3] suggested an efficient E-voting system in his article as fallows. A traditional voting system can be time consuming and cumbersome and takes a lot of time. With the growing development of Information Technology an E voting system tends to overcome all these limitations. E- voting is fast and helps us to cast our vote from any location. One of the main focus of then E-Voting System is security. In this paper he proposed an E-Voting System using Paillier Homomorphic Encryption Scheme which is used to provide security to the voting system and in turn help us to modify and transfer data in the encrypted form making it impenetrable. Here he uses the Paillier Encryption Homomorphic property that allows us to add the votes in encrypted form. The online vote casting systemis more reliable than the traditional system and is able to save to save the time

III. PROPOSED SYSTEM

The Paillier Cryptography is a modular, public key encryption scheme, created by Pascal Paillier, with many interesting properties. This paper will explore the improved or enhanced Paillier's work by concatenating the concept of the cryptographic Thresholding, Which distributes the process amongst a number of parties such that a message can only be decrypted if a certain qualified subset of these parties participates in the decryption method. The cryptosystem that supports such a process is called a threshold cryptosystem. It is assumed that the reader is familiar, to some degree, with modular arithmetic, as well as the concept of converting an alphanumeric message into a purely numeric message. Also, the term plaintext will be used to refer to a message that is numeric, but is not encrypted, while the term cipher text will be used to refer to plaintexts which have been encrypted, but not yet decrypted. In order to illustrate the system's potential. We will initiate with the encryption process with the combination of the blowfish algorithm to output the encrypted stream called the cipher text. . It takes a variable-length key from 32 bits to 448 bits which makes it more feasible than other encrypting algorithms maintain its reliability and superiority parameters.

No attack is known to be successful against it. Since the security algorithms performance along with malleability forms a mandatory criterion. Since there doesn't exist yet known concept on the Paillier's algorithms that confronts the malleability and performance concept and makes the concept stupendous. Hence in supporting the idea we try to bring out a novel system that takes into measures both of two parameters.

The Praposed methodology is homomorphic encryption based on paillier encryption cryptography.
The proposed scheme is stated below.

A. Paillier Cryptosystem (1999):

The Paillier theme, 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 performs 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 large primes p and Q

specified: gcd(pq,(p-1)(q-1)) = one In other words 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 gas n+1Compute 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 and r is 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)

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) = 20*12 = 240 mu = lambda^-1 mod n = 120^-1 mod 143

m = L(9636^120 mod 143^2) * (120^-1 mod 143) mod 143

m = 50

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

1) 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)

2) 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)

3) Algorithm

1) Step 1: Process of Key Generation takes place by using following

Produce two large prime numbers a and b randomly which are independent of each other such that gcd(a*b,(a-1)*(b-1)) = 1.

Calculate n = ab and k(n)= lcm(p-1,q-1) where k(n) being Carmichael function.

Select the generator g such that g belongs to Zn2

Compute the follow Modular Multiplicative inverse u = (L(gkmod n2))-1 mod n where L(u) = (u-1)/u So Pair of Key Generated: the public key is (n,g) and the private key is (k,u).

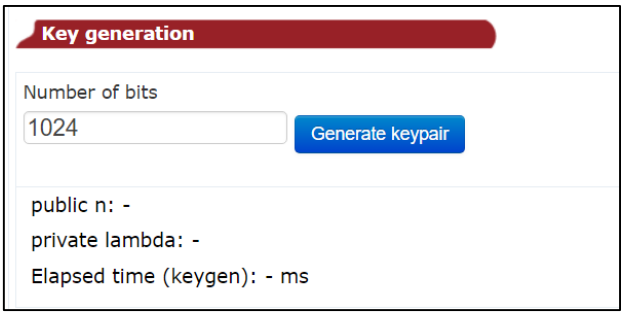
2) Step 2: Encryption Process

1) The message m is need to be encrypted where m belongs to Z
2) Choose a random number r
3) Compute cipher text c = gm * rn mod n2

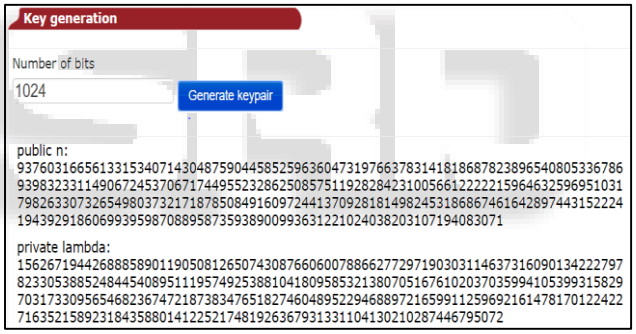
3) Step 3: Decryption Process

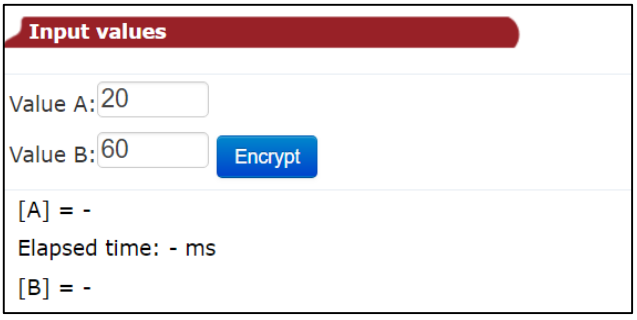
1) Cipher text c will be decrypted to get message m as follows by using private key (k,u) :- m = L(ck mod n 2) * k mod n

IV. RESULTS AND ANALYSIS

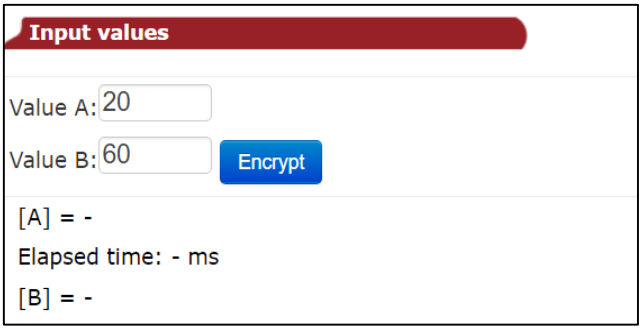


A. Key Generation

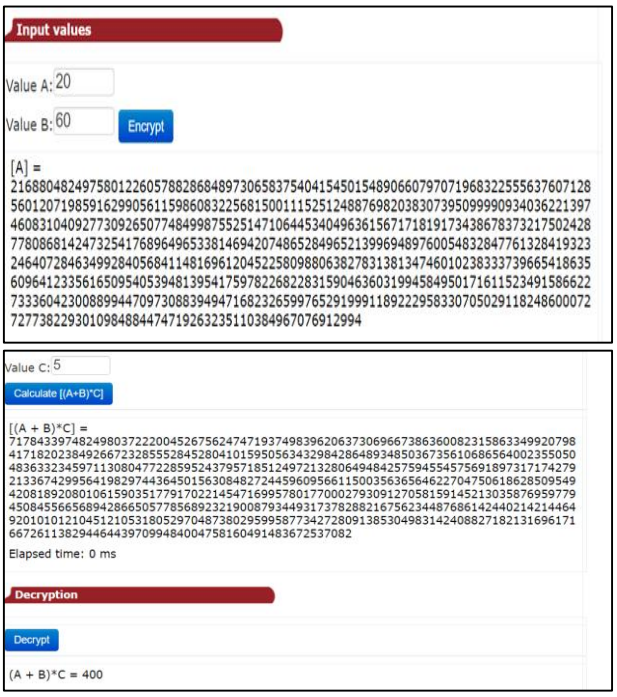




B. Encrypting the input values



C. Decrypting the message and getting the results



V. CONCLUSION

Security or privacy on fully Homomorphic encryption is a traditional concept on security which enables us to provide the encrypted data without knowing the prime entries on which the calculation was carried out respecting the confidentiality of data. However, our work is depends on the application of Homomorphic encryption which enables us to derive the security of the data and also its performance issue. As it is evaluated in the graphs of the malleability and performance itis evident that our algorithm provides a novel result which isfound to be good making the security of the Paillier's algorithm much compact and flexible. And Finally This paper carried out the Enhanced performance of Homomorphic Encryption based on paillier's cryptography.

REFERENCES

[1] Payal V. Parmar, "A Survey Of various Homomorphic encryption Schems,Vol.91-No.8, April-2014. International Journal of Computer Application(0975 – 8887)
[2] Pramod Kumar Siddharth, "A Homomorphic Encryption Scheme Over Integer Based On Carmichael's Theorem", 2016 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT) .
[3] Tannishk Sharma, "E-Voting using Homomorphic Encryption Scheme", International Journal of Computer Applications (0975 – 8887) Volume 141 – No.13, May 2016.
[4] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Advances in Cryptology (EUROCRYPT '99), vol. 1592 of Lecture Notes in Computer Science, pp. 223– 238, Springer, New York, NY, USA, 1999." .
[5] Craig Gentry and ShaiHalevi, "Implementing Gentry's fully- homomorphic encryption scheme," Advances in Cryptology– EUROCRYPT 2011, pp. 129– 148, 2011.
[6] Mads Johan Jurik, the Paillier Cryptosystem withApplications to Cryptological Protocols, BasicResearch in Computer Science, ISSN 1396-7002August 2003.
[7] Caroline Fontaine and Fabien Galand, Review Article "A Survey of Homomorphic Encryption for Nonspecialists" CNRS/IRISATEMICS, Campus de Beaulieu, 35042 Rennes Cedex, France, 24 October 2007.

