International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Ensuring Efficient Data Storage using Fully Mature Homomorphic Encryption Technique in the Cloud Environment

C.Saravanabhavan, K.Anguraju, M.Kannan, P.Preethi, R.Asokan

Abstract*: In cloud computing, user database is stored at remote site instead of user computer's hard disk where the connection between remote site and user computer is provided by internet connection. As cloud computing essentially places data outside the custody of owner of data, it inexorably hosts security disputes. The distance among the physical and the client location of data generates a barrier as the data can be accessed by an unauthorized party and this would influence the solitude of client's data. The utilization of traditional encryption systems to encrypt the data prior to transmitting to the cloud provider has been most extensively utilized technique to link this security gap. Be that as it may, the customer will require offering the private key to the server to unscramble the information in front of playing out the figuring's fundamental. Homomorphic encryption techniques permits computations on encrypted data devoid of decryption. This paper deals with the utilization of Fully Mature Homomorphic Encryption (FMHE) to encode the client's data on cloud server and as well it facilitates to perform required computations on the encrypted data.

***Keywords* : Computing Block, CryptDB, Homomorphic, Packet Channels**

I. INTRODUCTION

This is an International reputed journal that published research articles globally. The cloud computing is described as the computation in the cloud is a set of network permitted services offering expandable, quality of service assured, usually customized, cheap evaluation platforms based on the requirement which can be employed in an effortless and prevalent manner. Simply the cloud computing is the aggregation of technology, a platform which offers hosting and storage as a service over the internet. The intention of cloud computing is focused on offering expandable and cheap on-demand computation service structures with improved levels of service.

Revised Manuscript Received on 30 July 2019.

***** Correspondence Author

C.Saravanabhavan, Kongunadu College of Engineering and Technology, Trichy

K.Anguraju, Kongunadu College of Engineering and Technology, Trichy

M.Kannan , Kongunadu College of Engineering and Technology, Trichy

P.Preethi, Kongunadu College of Engineering and Technology, Trichy

R.Asokan, Kongunadu College of Engineering and Technology, Trichy

As these features might introduce diverse issues to the cloud computing system so the intention is to address these possible threats prevailing within the cloud computing environment.The quickly developing correspondence and processing innovation takes a jump with digitization of information in huge scale condition, in this way the need of gathering, breaking down and putting away

of colossal information ends up being a basic factor. Distributed computing innovation offers a capacity stage for a lot of information from various elements and encourages important information calculations. One of the real difficulties in such stage is to guarantee security and protection of information. The sender outsources the processed figure content to the remote server's site that altogether presents the risk of uncovering the information (Y. Chen et al; 2012). Because of absence of practical executions of different figure content calculation, sender may be repudiating from obtaining the goal by scrambling the information. Along these lines, the customary cryptosystems used for distributed storage needs figure content decoding in Cloud service providers' site. Privacy of the cloud data users [process, manage and store] are increased and manipulated to make the cloud framework more efficient with the standard Homomorphic encryption scheme is the challenging query while going with cloud.

Homomorphic encryption gives answer for this crisis, in which it performs calculations specifically on figure content. Homomorphic Encryption can be ordered into two gatherings grounded on its figure content computational abilities, for example (a) Somewhat Homomorphic Encryption (SHE) and, (b) Fully Homomorphic Encryption (FHE). SHE satisfies added substance and multiplicative properties for understanding calculations as a constrained arrangement of tasks I. e., circuits of constrained profundity, while FHE delights these properties for subjective profundity of the circuits. Upper class have proposed the development of FHE from SHE utilizing bootstrapping (C. Nobility et al.;2009)

This work envisions an effective and down to earth Fully Mature homomorphic cryptosystem for parallel usage of secure information stockpiling in cloud (C. Nobility et al.;2010). In this way, parallel and successive execution calculations for assorted benchmark figure content calculation, such as looking through a scrambled record, and modulus, division, square root, and so forth on figure text(C. Upper class et al.;2012). The base of this approach is the usage of multi-threading and "figure content revive" method execution at key age server (KGS).

The emergency looked in distributed computing can be comprehended by the Fully Homomorphic Encryption as it gives best answer for secure the

customer information in distributed computing since it can perform discretionary calculations on scrambled information without unscrambling. Also, it tends to the secrecy issues when information is shared by different clients and performs distinctive activities in a cloud (William Puech et al.; 2011), to specifically work on encoded information, dissecting the information and gives security et al.

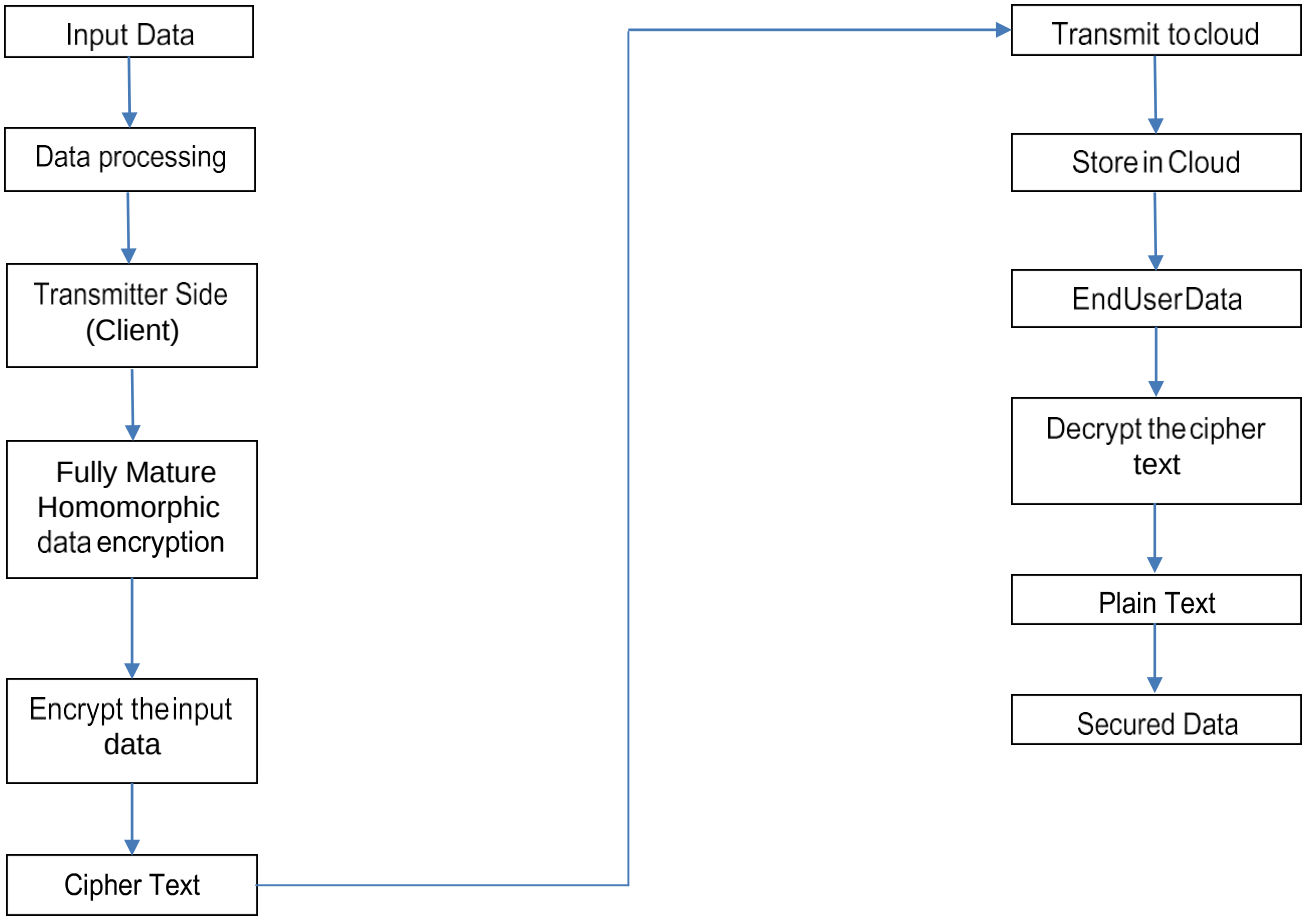


Fig. 1: Flow Diagram of Proposed FMHE Technique

II. LITERATURE REVIEW

A. Significance of Homomorphic Algorithm in providing Cloud Security

The following sub sections deliberate the role of Homomorphic Encryption scheme in providing security to the cloud in various ways:

B. Fully Homomorphic Encryption System (FHES)

Homomorphic encryption is an uncommon type of encryption by which one can play out a particular logarithmic task on the plain-message by applying the same or distinctive activity on the cipher text. On the off chance that X and Y are two numbers and 'E' and 'D' indicate encryption and decoding capacity, individually.

It worth saying that (Aguilar-Melchor, et al.; 2013) gives a methodical clarification of the new wording identified with FHE, where they don't present the HE plans and executions in detail.

Eventually, the raised prevalence of cloud based services rush the plan of HE frameworks which can keep up a self-assertive number of homomorphic activities with irregular capacities, i.e. FHE. Upper class' FHE conspire is

the principal conceivable and achievable FHE plot (Gentry; 2013). It depends on perfect cross sections in math and it isn't just a depiction of the plan, yet additionally an effective system for accomplishing FHE.

A HE strategy can utilize the comparable key for both encryption and unscrambling (symmetric), it is likewise intended to push off the different keys to scramble and decode (uneven). A bland strategy to change symmetric and deviated HE frameworks to each other is built up in (Gentry et al.; 2010).

C. Fully Homomorphic Encryption for Binary Bits

The fully homomorphic conspire (Ferrer, J.D et al.;2002) is a rearrangements of a prior work including perfect ideal lattices (Gentry; 2009). It scrambles a solitary piece (in the plain-content space) to an integer (in the figure content space).

The FHES of (Vizer, D., et al.;2015) works both over parallel and whole number numbers. This plan can perform both multiplication and addition tasks over the cipher-text and these activities are spoken to in plain-text.

Consequently, an untrusted party can work on private or secret information, without the capacity to realize what information the untrusted party is controlling.

RSA is halfway homomorphic cryptosystem as its multiplication attributes of a completely homomorphic encryption (Manish M Potey et al;2016), by the by completely homomorphic encryption ought not persuade the increase qualities but rather the expansion qualities. Therefore, the extra calculation influences it to gain the expansion attributes of full homormorphic encryption (Phillip Burtyka,;2014). To sum things up, the proposed framework has two answers for alter RSA calculation to make the changed RSA calculation to fulfill homomorphic encryption calculation.

D. Fully Homomorphic Encryption for Integers

Secure intrigue gather arrangement manages the protection and security of some numeric esteems being traded between the customer and the server. Along these lines the basic cryptosystem must be stretched out to oblige whole number numbers with the goal that number numbers can be contemplated (Stehlé, D et al.; 2010). This objective is accomplished by speaking to the whole number as a paired vector and scrambling each piece independently and keeping up their positions or requests.

FHE offers capability of executing scrambled information calculation; it anticipates various stand up to for doing the calculations which executes over encoded information (Zuowei et al.;2017). Neverthlessly, the emergency associated with deciphering direction executions, loops handling, variable definitions, and conditions ending when calculations managed the encoded information and scrambled controls.

The focused on completely homomorphic encryption framework that gives three components to ciphertexts and two elective techniques for decoding. This plan is the most effective focused on fully homomorphic cryptosystem (O. Regev et al; 2009).

E. Partially Homomorphic Encryption Schemes

RSA is an early case of Partially Homomorphic Encryption and presented by Rivest, Shamir, and Adleman (Rivest et al.; 1978) not long after the creation of public key cryptography by Diffie Helman (Diffie and Hellman; 1976). RSA is the primary possible accomplishment of general society key cryptosystem.

F. Somewhat Homomorphic Encryption Schemes

The foreseen properties of cryptosystems' homomorphism were limited either by multiplication or addition process i.e., SWHE technique. The critical advances play out a FHE conspire was started by Boneh-GohNissim (BGN) in (Bendlin, R et al.; 2011). It gives a self-assertive measure of increases and one multiplication by putting the consistent figure content size.

A SWHE framework can assess the cipher text homomorphically for a predetermined number of activities. In the wake of thresholding, decryption capacity neglects to recover the message from cipher text precisely. The entirety of noise in cipher text ought to be diminished to adjust the loud CT to a proper cipher text.

A Tweaked SWHE (Gentry; 2009) started changes to SomHom to shorten decryption algorithm for developing fully homomorphic framework. The changed framework SomHom differs from unique plan in the key age stage and decryption calculation (Stehle and Steinfeld;). Two improvements to Gentry's plan, that reductions the measure of vectors in SSSP occurrence, and another can be used to diminish the decoding polynomial degree (presenting a little likelihood of unscrambling mistakes).

(Paulo Martins et al.; 2017) suggested that a programmer can bargain delicate information that is put away in a scrambled frame. In any case, when information is to be prepared, it must be decoded, getting to be powerless against assaults. Homomorphic encryption settles this weakness by enabling one to compute straightforwardly on encoded information. In this study, both past and current Somewhat Homomorphic Encryption (SHE) plans are checked on, and the all the more effective and late Fully Homomorphic Encryption (FHE) plans are completely examined. The ideas that help these plans are introduced, and their execution and security are investigated from a building angle.(Zuowei et al.; et al, 2017) depicts that to enhance the effectiveness of the current homomorphic encryption strategy, in view of the DGHV conspire, an enhanced completely homomorphic plot over the whole number is proposed. Under the commence of guaranteeing information proprietor and client information security, the plan underpins the expansion and increase activities of ciphertext, and guarantees speedier execution effectiveness and meets the security prerequisites of distributed computing. Security investigation demonstrates that our plan is protected. Execution evaluation shows that our plan would more be able to proficiently actualize information than DGHV conspire.Phillipp Burtyka et al; 2014) proposed another completely homomorphic encryption (FHE) conspire. Dissimilar to past ones, our FHE conspire is viable and sufficiently straightforward for pragmatic applications. Our FHE basically abuses scientific group of framework polynomials which are grid conditions of a specific shape. This makes the plan both quicker and (we trust) less demanding to comprehend than precursors. Additionally, the paper gives the formal meanings of new system for secure distributed computing - the crude of minimal symmetric completely homomorphic encryption conspire whose security depends on the trouble of some NP-finish issue. We consider associationand foundation of secure cloud calculations utilizing such symmetric completely homomorphic encryption.

Development of the proposed encryption conspire presents another hardness supposition. Some fundamental thoughts clarify the security of such FHE against known plaintext assaults. We give hypothetical assessment of plan's overhead (both in time and size).

The paper gives exploratory examination on fully homomorphic encryption of our write. Our usage utilizes NTL library by Victor Shoup, and we display a genuine effectiveness of the encryption conspire.(Manish M. Potey et al; 2016) bases on securing data on

the cloud in the encoded sort out using totally homomorphic encryption. The data is secured in DynamoDB of Amazon Web Service (AWS) open cloud. Customer's count is performed on encoded data with no attempt at being subtle cloud. Exactly when comes about are required they can be downloaded on client machine. In this circumstance customers data is never secured in plaintext on open cloud.

(Khalil Hariss et al, 2018) propose another proficient symmetric lightweight Fully Homomorphic Encryption calculation, called "NOHE", which benefits from the effortlessness of the rationale NOT and the homomorphic conduct of Morgan Theorem. The proposed calculation is clarified in detail and assessed. The security execution comes about demonstrate a satisfactory execution time with no capacity overhead and high resistance to assault.

(A.M. Vengadapurvaja et al; 2017) portrays that Fully Homomorphic Encryption plot underpins both totaling and multiplication. The input images and the comparing encoded pictures are appeared. The DICOM image is the input image. The investigation like keyspace examination, Key affectability investigation, histogram analysis, correlation investigation, PSNR and MSE analysis, Noise analysis are achieved. The chance of lessening Recrypt by investigating the normal blunders acquainted due with wrong examinations, which emerge because of the expulsion of the de-noising step. Results demonstrate that reasonably picking the quantity of Recrypt activities brings about a relatively arranged exhibit (Ayantika Chatterjee, 2013). This rouses to build up a two-organize arranging called LazySort: the principal stage playing out a Bubble sort with diminished Recryptoperations to bring about a relatively arranged cluster, to be trailed by a moment organize which utilizes an Insertion sort with all Recrypt activities. Point by point tests demonstrate that gets a huge accelerate in the arranging time.

Dynamic multi keyword oriented search Algorithm is recommended that contain adjusted fully homomophic encryption and prims Algorithm. In view of catchphrase recurrence show in the record, watchwords are arranged and fabricated accessible file for watchword and documents (D. Palanivel Rajan; 2017). The dynamic tree is developed utilizing tidy's calculation in view of watchword and document. The encoded records of the tree are listed to catchphrases utilizing two way Hash table for productive pursuit and retrieval of reports. The documents are scrambled utilizing adjusted ringbased completely homomorphic encryption. The exploratory outcome demonstrates that planned wok gives 80% and 86% encryption and unscrambling throughput and set aside less ordering opportunity to record the documents than standing RC4+.

G. Biometrics and homomorphic encryption

In a homomorphic encryption technique, biometric included data is disguised by encryption, and the two element information closeness is estimated on encoded information (Park,; 2011). In particular, closeness figuring is accomplished on scrambled information, differing from traditional encryption strategy in which correspondence channels information are encoded (Luna, J; 2016), however likeness computation is done on plaintexts after unscrambling. This technique makes a biometric conspire "cryptographically secure" as long as the mystery key is taken care of by the confided in party.

Algorithm	Public Key	Secret Key	Cipher Key
Gentry	$n7$	$n3$	$n1.5$
BGV	$2an. \log q$	2a. log q	2a. $\log q$
MORE	NA	$O(2\lambda)$	$O(2\lambda)$
Improved Gentry	$\tilde{O}(\lambda 3.5)$	$\Theta(\lambda 1.5)$	$\tilde{O}(\lambda 3.5)$
BV	$O(n2 \log 2\ q)$	$n.\log q$	$(n+1).\log$ q

Table I: Sample Representation Of Algorithm Performance

III. HOMOMORPHIC ENCRYPTION SCHEMES

A. BGV Encryption Scheme

Overseeing number vectors (whose security is dependent on the hardness of decisional LWE (Learning with Errors) and dealing with the entire number polynomials (whose security is liable to the hardness of the decisional R-LWE (Ring LWE) are two variations of the cryptosystem. BGV is an uneven encryption plan which can be used for the encryption of the bits (Khalil Hariss et al; 2017).

B. Gorti's Enhanced Homomorphic Cryptosystem (EHC)

EHC is the new Enhanced Homomorphic Cryptosystem utilized for homomorphic Encryption/Decryption with secure information exchange. There are various uses of this kind of homomorphic encryption in the continuous. Homomorphic encryption has some key idea that the framework will complete the calculations on the beforehand encoded information without knowing about its genuine esteem. At last, this processed encoded information or message will be sent back as a result and unscrambled. This decoded result must be equal to the expected registered esteem if obtained on the genuine data. For this reason, a particular structure must be offered by the encryption framework (Gorti VNKV Subba Rao, 2013).

C. Algebra Homomorphic Encryption Scheme

This procedure is the changed model of advanced mark standard DSS offered by NIST in America. The AHEE security is the most elevated amount of the security. Added substance homomorphism alludes the comparable 'k' for encryption however makes utilization of the irregular number 'k' in E1 () which relates AHEE ready to contradict plaintext assault. The AHEE goes about as the completely homomorphism subsets. AHEE has been validated to be more secure. This clarification of completely homomorphism is exceedingly created by Rivest, Adleman and Dertouzos.
Dangers of physically catching automatons and assaulting channels have been explored by numerous scientists.

These risk examinations and countermeasures are valuable to create shields against airborne assailants. At that point the following regular focus of assault is the controller, particularly specified that most automaton applications will entail some level of self-rule (Jung Hee Cheon, 2018).
In any case, there has not been much thought about the security of controller itself. On the off chance that the mystery keys of controllers are stolen, the entire framework can progress toward becoming administered by pernicious assailants.

IV. SECURITY ENHANCEMENT USING HOMOMORPHIC ENCRYPTION

Security is the premier need as the expanding routine with regards to web or public cloud for amassing the data. Security is basic for ensuring the privacy, respectability, accessibility of assets to offer data framework. The information can be put away in the scrambled organization in the database however the activities or calculations over the encoded information are important to be executed also, it is basic to decode the information yet unscrambled information are not ensured any more in this custom, a clever thought of cryptosystem permits the immediate figuring on encoded information. This thought is known as security homomorphism. In any case, unscrambling isn't executed; the result gained is comparable as computations over plaintext.

Perils of physically getting machines and striking channels have been explored by different experts. These danger examinations and countermeasures are beneficial to make shields against airborne aggressors. By then the going with run of the mill point of convergence of strike is the controller; particularly given that most choke out applications will require some degree of independence. Regardless, there has not been highly contemplated the security of controller itself. In the event that the mystery keys of controllers are stolen, the entire structure can progress toward getting the chance to be addressed by risky aggressors.

The structure (Jung Hee Cheon; 2018), where controllers don't have to stay discreet keys used to encode messages presented the machine by using homomorphic affirmed encryption, has two or three reasons for interest. It verifies the controller itself, and keeps from listening stealthily and mutilation assaults. Likewise, no persuading inspiration to stress over copy, lost, or stolen keys improves adaptability and empowers wide scale approaches. In addition, the course that there is no decoded part in the controller refreshes transportability of the thing and makes it adaptable in different stages and client conditions, and offering assurance when gained by an adversary.

Security is required to ensure web and cloud organizations. At the customer level, one needs to perform trust course of action and reputation add up to over all customers. At the application end, we need to set up security prudent steps in worm control and intrusion disclosure against disease, worm, and circled DoS (DDoS) attacks. It is basic to pass on parts to dodge online burglary and copyright encroachment of automated substance. Consider about reputation structures for guaranteeing cloud systems and server ranches. Security obligations are divided between cloud providers and customers unmistakably for the three cloud advantage models. The providers are completely accountable for arrange availability. The IaaS customers are more responsible for thecharacterization issue. The IaaS providers are more responsible for data reliability. In PaaS and SaaS administrations, providers and customers are likewise responsible for sparing data honesty and mystery.

In light of the cloud data security issue went up against, the homomorphic encryption part, displays a conveyed figuring data security framework. The arrangement ensures the transmission data between the cloud and the customer framework. Likewise, in the appropriated stockpiling their data is so far secured. It is useful for customers and the pariah association to look for date to orchestrate.

V. RESEARCH METHODOLOGY AND SPECIFICATION

A. Tools

The benchmark Fully Mature Homomorphic Encryption models will be produced in MATLAB by methods for the settled direct tool compartment toward do the fundamental whole number- crunching. Relentless upgrades in method require the capacity to quickly execute in a high level language like MATLAB.

For example, this work thinks about information (datasets) from Google drive to complete the Fully Mature Homomorphic calculation. Google Drive is in excess of a cloud-based capacity and matching up benefit. It too exceeds expectations at giving us a chance to make, store, alter, and team up the archives. The administration is really moving in exactly how far it goes to help you deliver and alter records, regardless of whether you are running solo or as a major aspect of a group.

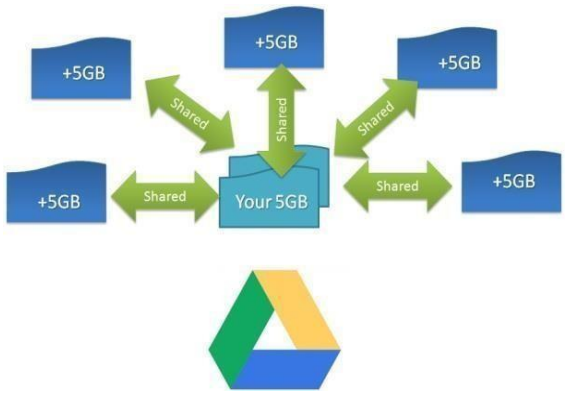


Fig. 2: Google Drive data cloud storage tool

There are a few mysteries to achieve the most out of Google Drive and the buddy applications Google Sheets, Docs, and Slides. In any case, there is slight inquiry that it is one of the sweetest cloud commitments you can discover.

Moreover,it's free-unless we require putting away more than 15GB of records not created with the online applications.

Google Drive is allowed to use with a Google record, and it shows up with a liberal 15GB of free stockpiling. Documents made with Google Sheets, Docs, and other in-Drive applications (in Google's restrictive, online configurations) don't tally toward the quantity, nor do records imparted to you. We can peaceful of fare these documents to higher standard configurations, so it's quite misfortune.

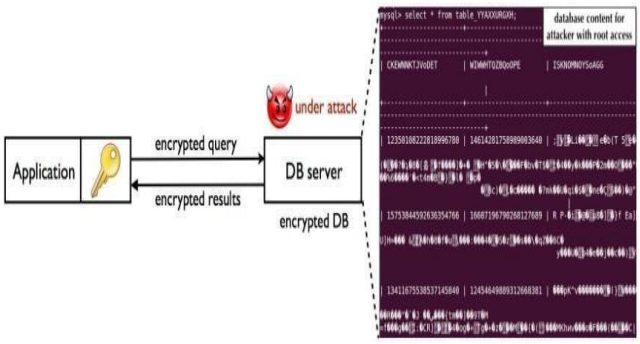


Fig. 3: Internal Functionality In Cryptdb

B. Proposed implementation

The encryption procedure is homomorphic identifying with the boolean circuits with addition and multiplication mod 4. The framework 'S' contains four procedures as Key Generation, Encryption, Decryption and Evaluate. The Evaluate input parameters, for example, open key puk, circuit 'C' and ciphertext tuple {c1, . . . , ct} as info and give another ciphertext 'c' as result.

The plan S=(KeyGen, Encrypt, Decrypt, Evaluate) is FullyMature homomorphic for issues 'P' of circuits for all circuits C x C. 'ε' is completely homomorphic on the off chance that it persuade every single boolean circuit. Circuit-protection and thickness are two huge properties of homomorphic encryption framework.

Circuit security banters the property of ciphertext change by Evaluate, ought not give anyidea concerning the plaintext that assess in front of the yield estimation of that circuit until the point when the customer finds out about the private key. Smallness expresses the property that ciphertext prepared by Evaluate should not to depend on the circuit C.

The security of completely homomorphic encryption framework has been broke down by methods for whole numbers while picking ciphertext assault demonstrate. The chose ciphertext assault copy is an exemplary security models as much as an encryption conspire is concerned. A ciphertext assault that breaks the security of plan is worried here. Also, the picked ciphertext assault lies on the subsistence of decoding that may not always exist. In this work, decoding can be developed by methods for response assault of a completely homomorphic encryption conspires that are used in an outsourcing computing condition.

C. Encryption process

First the plaintext is grouped and the group length is sensed based on the demand of security provided to the cloud (Tang J et al; 2016). Subsequently all the plain text group is encrypted using the fully mature homomorphic algorithm (Maha Tebaa et al, 2012). The following are the steps for encryption:

To begin with the plaintext is gathered and the gathering length is detected in light of the request of security gave to the cloud (Tang J et al; 2016). In this way all the plain content gathering is scrambled utilizing the completely develop homomorphic calculation (Maha Tebaa et al, 2012). The accompanying are the means for encryption:

1) Arbitrary prime number P has been chosen, and fixed and security prime number Q is chosen (length of P > length of Q > length of plaintext group);

2) Assemble the plaintext X where the length is L (L's number of digits is less than P), X=x1x2x3…xt;

3) Produce the random number R;

4) Use the fully mature homomorphic encryption algorithm ci=xi + P + R x Q to calculate the ciphertext, where C= c1,c2,c3..ct;

5) Direct the ciphertext C towards the receiver.

D. Decryption process

1) The receiver obtains the ciphertext C, and groups the cipher text C= c1c2c3…ct;

2) Use the key P and the decryption algorithm xi=ci mod P to compute xi;

3) Finally, the plain text X is obtained.

The security prime number Q is a fixed number and it is given to the cloud server.

The fully mature homomorphic encryption is homomorphic for totaling and multiplication.

E. Retrieval process

1) The key is encrypted, and acquire a short cipher text ck initially. As known, cg is the cipher group,

Cg = xi + P + R1 x Q;

Ck = key + P + P x R2 x Q;

2) For each group ci, result = (cg – ck) mod Q = (cg – key + P × Q × (R1 – R2)) mod Q = cg – key

3) If comaprison is positive, the outcome is "0"

Cloud planning security challenges are in addition an issue to a couple of investigators; beginning need was to focus on security which is the best worry that is perceived a transition to the cloud. Our recommendation is to offer the arrangement to execute the calculating calculation on the encoded data in the cloud with no learning got to the cloud authority center. This work attempted to achieve the totally homomorphic encryption which can execute endless number juggling exercises on the ciphertext.

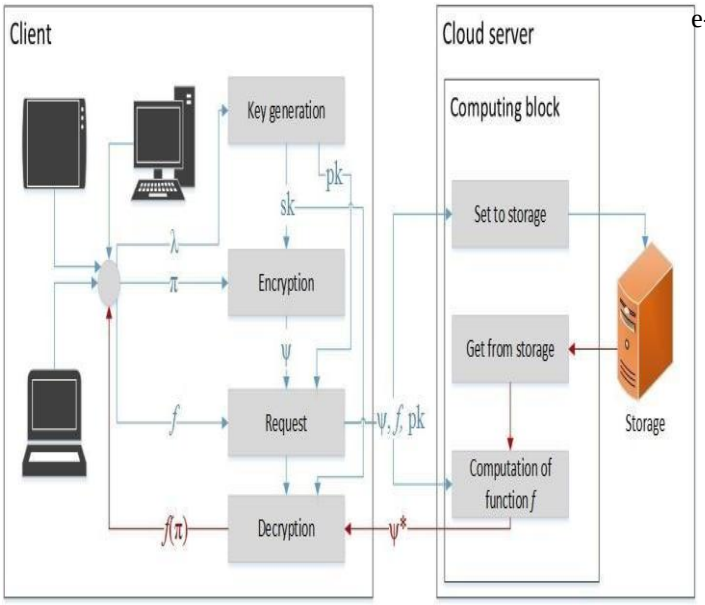
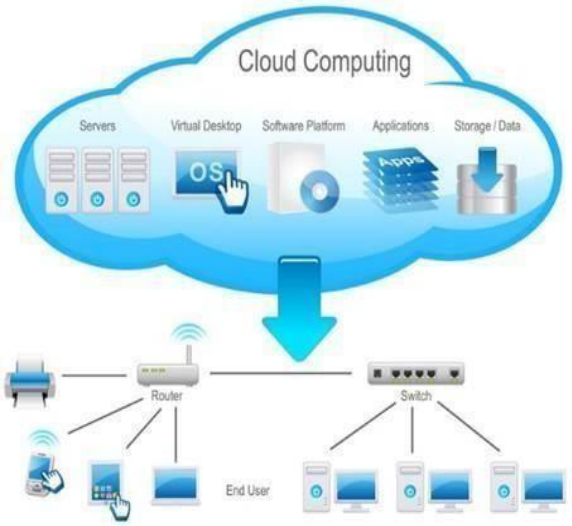


Fig. 4: Block diagram of Fully Mature Homomorphic algorithm

VI. EXPERIMENTAL RESULTS

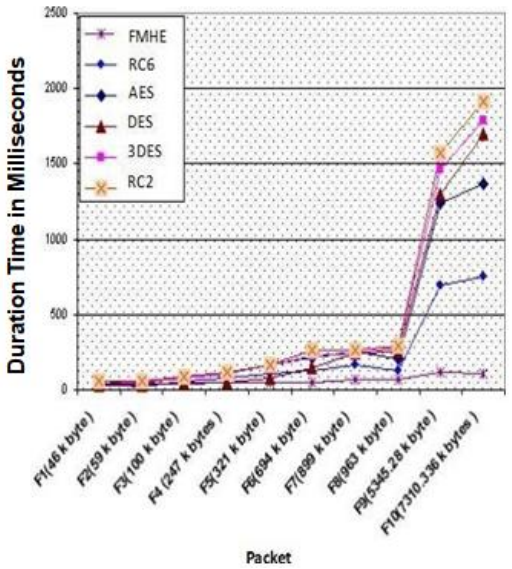
Graph 1 speaks to the Encryption of Different Packet Size Encryption time which is utilized to ascertain the throughput of an encryption conspire. The throughput of the encryption plan is determined by partitioning the all-out plaintext in Megabytes encoded on the absolute encryption time for every calculation in. As the throughput worth is expanded, the power utilization of this encryption method is diminished.

The results in graph 2 shows the predominance of FMHE over different calculations as far as the preparing time. Another point can be seen here; that RC6 requires less time than all calculations with the exception of FMHE. A third point can be seen here that AES has a bit of lee way over different 3DES, DES and RC2 as far as time utilization and throughput. A fourth point can be seen here; that 3DES has low execution as far as power utilization and throughput when contrasted and DES. It generally requires additional time than DES due to its triple stage encryption attributes.

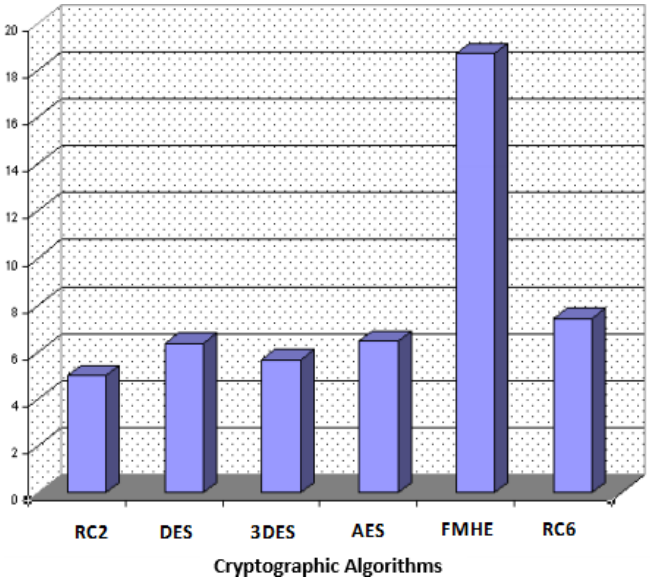


At **Fig. 5: Proposed Implementation Diagram**

last, it is discovered that RC2 has low execution and low-throughput when contrasted and other five calculations disr e-garding the little key size utilized.



Graph 1: Time Consumption Comparison (From Cloud Sim Tool)



Graph 2: Throughput Comparison (From Cloud Sim Tool)

VII. HELPFUL HINTS

The below table II represents the missing features of some existing algorithms and techniques in terms of ensuring security in cloud environment.

S. No	Title	Key features	Results	Missing features
1	Employing Gentry's Fully- Homomorphic Encryption Structure	Key-age method for the hidden to some degree homomorphic encryption, that does not require full polynomial reversal	Open key size ranges in size from 70 Megabytes for the "little" setting to 2.3 Gigabytes for the "enormous" setting	It turns towards insecurity
2	Secure and productive online information stockpiling and sharing over cloud condition utilizing probabilistic with homomorphic encryption	To keep up nature of administration and improve consumer loyalty yield better encryption strategies decrease security assaults, expanded throughput	When transmitting 001–100 mb of data the Null encryption takes more time to execute The data size is 854 MB which have the null encryption of 343.15 ms, the data is encrypted with the probabilistic algorithm to give the throughput of 326.26 ms	Fast execution time diffusing only in partial data.
3	Homomorphic Encryption for preserving the Safety of Cloud Data	Data is deposited in DynamoDB of Amazon Web Service (AWS) civic cloud	It gives privacy to the information as in no stage information is uncovered in plain content. The proposed calculation is rearranged, productive form connected in AWS open cloud	To advance different calculations for looking and questioning on scrambled information under FHE

Retrieval Number: B2265078219/19©BEIESP
DOI: 10.35940/ijrte.B2265.078219
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

4	Intermediary re-encryption architect for putting away and sharing of cloud substance	A secure file imparting system for the cloud to intermediary re-encryption (PRE)	Execution improvement in framework dependability, uprightness, and security	Cloud storage should be performed in various cloud datasets
5	Using Fully Homomorphic Encryption to Shelter Cloud Computation	Homomorphic encryption permits to achieve computations on encrypted data deprived of decryption	Accomplish arbitrary calculations on encrypted data deprived of decrypting for improved security	Cloud computing and analysis the complexity of the scheme
6	Fully Homomorphic Encryption with Comparatively Minor Key and Ciphertext Magnitudes	Scheme has smaller message extension and key scope than Gentry's original scheme	To some degree homomorphic scheme the public and private keys comprise of two enormous whole numbers (one of which is shared by both the public and private key) and the ciphertext comprises of one enormous number.	Still no deep performance to empower completely homomorphic encryption; in any event at down to earth key sizes.
7	Ensuring Efficient Data Storage Using Fully Mature Homomorphic Encryption Technique In The Cloud Environment	Perform FMHE in datasets to prove the efficiency	Will proved higher security and confidentiality amongst the data	To be tested under various datasets

Table II. Comparison of various encryption techniques with the proposed technique.

VIII. CONCLUSION

Fully Mature Homomorphic Encryption conveys another view point to distributed storage. It offers privacy to the information as when information is uncovered in plain content. The anticipated algorithm is rearranged and capable for all variant connected in cloud. The projected calculation can be used for differing applications like medicinal purposes, auctioning through online and business purposes. The need to perform investigate in diminishing the cipher text size for proficient information preparing can be utilized through FMHE algorithm. Also, the same technique can be applied to encode and decode different. Thereby data distribution become secured in unsecure network channels and it makes the user to easily share important files and maintaining data integrity.

ACKNOWLEDGMENT

We would like to show our gratitude to Dr.PSK.R.Periaswamy, Chairman, Kongunadu Educational Institutions, for providing resources in terms of infrastructure to complete this research work within the stipulated period of time.

REFERENCES

1. Aguilar-Melchor, C., Fau, S., Fontaine, C., Gogniat, G., Sirdey, R.: Recentadvances in homomorphicencryption: apossiblefuture. IEEESignal Process. Mag. 30(2), 108–117(2013)
2. Van Dijk, M., Gentry, C., Halevi, S., Vaikuntanathan, V.: Fully homomorphic encryption over the integers. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 24–43. Springer, Heidelberg (2010).
3. Ferrer, J.D.: A provably secure additive and multiplicative privacy homomorphism. In: Chan, A.H., Gligor, V.(eds.) ISC 2002. LNCS, vol.2433, pp. 471–483. Springer, Heidelberg (2002).

4. Vizer, D., Vaudenay, S.: Cryptanalysis of chosen symmetric homomorphic scheme. Stud. Sci. Math. Hung. 52(2), 288–306 (2015)
5. Luna, J., Abdallah, C.T., Heileman, G.L.: Probabilistic optimization of resource distribution and encryption for data storage in the cloud. IEEE Trans. Cloud Comput. 6(1), 1–13. doi: 10.1109/TCC.2016.2543728
6. Park, N.: Secure data access control scheme using type-based re-encryption in cloudenvironment. In: Semantic Methods for Knowledge Management and Communication, pp. 319–327. Springer, Berlin (2011)
7. Bendlin, R.,Damgård, I., Orlandi, C., Zakarias, S.: Semi-homomorphic encryption andmultiparty computation. 'In: Advances in Cryptology–EUROCRYPT2011,pp.169–188.Springer,Berlini(2011)
8. Zhang, X., et al.:Privacypreservationoverbigdata in cloudsystems. In: Security, Privacyand Trust in CloudSystems, Springer, pp. 239–257 (2014)
9. Zhang, X., et al.: Scalable local-recoding anonymization using locality sensitive hashing for bigdata privacy preservation. In: Proceedings of the 25th ACM International on Conference on Information and KnowledgeManagement, pp. 1793–1802 (2016)
10. Liu,H.,et al.:Shared authority based privacy-preserving authentication protocol in cloud computing. IEEE Trans. Parallel Distrib. Syst. 26, 241–251 (2015)
11. Cao, N., et al.: Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE Trans. Parallel Distrib. Syst. 25, 222–233 (2014)
12. Kaaniche, N., Laurent, M.: Data security and privacy preservation in cloud storageenvironments based on cryptographic mechanisms. Comput. Commun. 111, 120–141 (2017)
13. Yu, Y., et al.: Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. IEEETrans. Inf. Forensics Secur. 12, 767–778 (2017)
14. Tang,J., et al.: Ensuring security and privacy preservation for cloud data services. ACM Comput. Surv. (CSUR) 49, 13 (2016)
15. Gentry, C., Sahai, A., & Waters, B. 2013. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Advances in Cryptology-CRYPTO 2013 pp. 75-92. Springer.
16. Yogapriya, J., Saravanabhavan, C., Asokan, R., Vennila, I., Preethi, P., Nithya, B. 2018. A Study of Image Retrieval System Based on Feature Extraction, Selection, Classification and Similarity Measurements. Journalof Medical Imagingiand Health Informatics, 8(3), 479-484.
17. Saravanan, K; Asokan, R; Venkatachalam, K., Neuro- Fuzzy Based Clustering of Distributed Denial of Service (DDoS) Attack Detection Mechanism, International Information Institute (Tokyo). Information; Koganei Vol. 16, Iss. 11, (Nov 2013).
18. Padmini Bai D and Preethi P, "Security Enhancement of Health Information Exchange Based on Cloud Computing System", International Journal of Scientific Engineering and Research, pp. 79-82, Volume 4 Issue 10, October 2016.
19. Vellingiri, J.; Balambigai, S.; Saravanan, K.; Asokan, R., Secure Real Time Web Based Electrocardiogram Monitoring System for Improved Healthcare, Journal of Medical Imaging and Health Informatics, Volume 6, Number 3, June 2016, pp. 774-778(5).
20. Preethi P, Asokan R, A High Secure Medical Image Storing and Sharing in Cloud Environment Using Hex Code Cryptography Method—Secure Genius, Journal of Medical Imaging and Health Informatics, Volume 9, Number 7 (September 2019) pp.1337 1546.

AUTHORS PROFILE

Dr.C.Saravanabhavan, Head of the Department in the Department of Computer Science and Engineering, Kongunadu College of Engineering and Technology, Trichy, Tami Nadu, India. He received M.Tech., from Sathyabama University, Chennai in 2007. He has 15 years of teaching experience and completed Ph.D., in Anna University, Chennai. His area of interest lies in Data Mining, Cloud Computing, Network Security and published 21 papers in international journals and presented 23 papers in national and international conferences in that area.

Mr.K.Anguraju, Assistant Professor in the Department of Computer Science and Engineering, Kongunadu College of Engineering and Technology, Trichy, Tami Nadu, India. He received M.E., from Vinayaka Mission KV Engineering College, Salem in 2013. He has 6 years of teaching experience. His area of interest lies in Networking, Data Mining, Cloud Computing and published 6 papers in international journals and presented 5 papers in national and international conferences in that area.

Mr.M.Kannan, Assistant Professor in the Department of Computer Science and Engineering, Kongunadu College of Engineering and Technology, Trichy, Tami Nadu, India. He received M.E., from Regional Centre, Anna University, Coimbatore in 2013. He has 5 years of teaching experience. His area of interest lies in Data Mining, Cloud Computing, Network Security and published 5 papers in international journals and presented 6 papers in national and international conferences in that area.

Ms.P.Preethi, Assistant Professor in the Department of Computer Science and Engineering, Kongunadu College of Engineering and Technology, Trichy, Tami Nadu, India. She received B.Tech., degree from Roever Engineering College, Perambalur in 2012. She was awarded with M.E., from Srinivasan Engineering College, Perambalur in 2014. She has 6 years of teaching experience and pursuing Ph.D., as part-time research scholar in Anna University, Chennai. Her area of interest lies in Cloud Computing, Network Security and published 11 papers (Annexure 1: 2 papers) in international journals and presented 13 papers in national and international conferences in that area.

Dr.R.Asokan, Professor / ECE & Principal, Kongunadu College of Engineering and Technology, Trichy, Tami Nadu, India. He has more than 30 years of teaching experience and 15 years of research experience. His area of specialization includes Wireless Networks, Image Processing. He has produced 10 Ph.D., scholars. He has published more than 100 papers in International Journals and presented more than 75 papers in National and International Conferences and published 1 book. He has obtained funding projects from various funding agencies. He is an Associate Editor in the Journal of Selected Areas in Telecommunications (JSAT)-Cyber journals. He is an Editorial Board Member in various International Journal. He has awarded 3 national awards. He is an active member of diverse professional bodies like IETE, ISTE, ACS, CSI etc.