International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Accelerating Information Security in Cloud Computing using a Novel Holomorphic Scheme

Dhananjaya, Balasubramani R

Abstract: ***In the past decades, many security algorithms are invented and used in many applications for encryption and decryption of information or data. All the secure algorithms were uses the security key of size 8bit, 16bit, 32bit, 64bit and 128bits for encryption and decryption but literature survey says that higher the key size, higher the security. But the higher key size has number more bits and its requires more memory for storage and also to perform each and every bit through computational operations leads to more delay. To address these issues, the key and plain text are of 128bits and converted into integer. The converted integer values of key and plaintext are encrypted and decrypted using Holomorphic through Advanced Encryption Standard (AES). The research method is sophisticated and more protected through meaning fully lesser key in size and is accomplished for encryption in terms integer key and plaintext moderately than binary bits, therefore larger size of key and plaintext can be minimized and reduced the computational complexities. Finally the cipher text is uploaded into cloud through Real Time Transport Protocol (RTP) and Real Time Transport Control Protocol (RTCP) for storage. The main problem with continuous sharing of information into cloud is security attacks so in this research work, three different multimedia signals such as ECG, EEG and biomedical images are converted into integer and encrypted using AES. The stored data can access by the authorized users and can decode the information after decryption using AES.***

Keywords **: *Multimedia data, AES, Cloud, IOT, thingspeack and RTP-RTCP.***

I. INTRODUCTION

The Scheme of Homomorphic Encryption bolster "handling the information though it is encoded". The exploration of theme that has picked up force subsequently Craig Gentry's first development of a Fully Homomorphic Encryption (FHE) plot dependent on arithmetical cross section hypothesis [1][2] introduced in 2009. This leap forward effort takes turned into an appealing arrangement, particularly related to security, protection issues of distributed computing pertaining to their applications. The FHE is mathematically homomorphic, supportive boundless increases and duplications of encryption output usually called as cipher text, because of which it achieves the capacity to figure discretionarily several capacity on the scrambled information [1-2, 5].

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author
Dhananjaya V*, Research Scholar, NMAM Institute of Technology, csdhananjay@gmail.com
Dr. Balasubramani R, Professor in ISE, NMAM Institute of Technology, balasubramani.r@nitte.edu.in

An underlying development of comprises FHE of a three stage diagram, which incorporates, 1) Developing a Somewhat Holomorphic Encryption plan that supports various additions and couple of growthes2) Squeezing the decoding capacity of the SHE, lastly 3) Procurement the FHE [5]. FHE plans as per Gentry's diagram [3-4,10] are wasteful and unfeasible in light of the immense among the complexities of the computational operations which can handle the cipher-text and the comparing plain-texts [11]. The real commitment for the high multifaceted nature is by enormous message development and the encrypted invigorating Decrypt technique amid the security. Focusing on the Gentry's plan and their variations, a limited works has accounted for amid the recent years proposing enhancements [6], development in the key age calculation [7-8][12, 16] and diminished open key size [8], innovative plans taking out the stage two of the discussed before outline [9], expansion to bigger message space and SHE that can assess low degree works productively. For some submissions by and by, a SHE plot, for example, the one proposed in this paper, is adequate for scrambled information preparing. The suggested public key by using holomorphic encryption system as an effective and commonsense can be considered variation for DGHV method of SHE is discussed in [4]. The $\tilde{O}(n^4)$ is suggested for the public key size and large mathematical multifaceted operations is $\tilde{O}(n^8)$. The original data is a ring i.e$\mathbb{Z}$R, here the number of bits 'n'. Its augmentation to whole number information for encryption or bigger missive interplanetary diminishes the original data development proportion from n^5 of the current plans to n3. Because of this, the various remainders and the related complexities required amid a circuit (or the comparing capacity) assessment are relieved. Generally, if a $\tilde{O}(n)$ bits whole number is scrambled, the enhancement in the productivity of circuit assessment is of a similar request. Likewise, the littler open key requires lesser extra room and system correspondence intricacy. The security of the projected plan depends on the difficult issue of tackling the two-component Partial Approximate Greatest Common Divisor (PAGCD), and the improvement in effectiveness of the plan is dissected to demonstrate its reasonableness [13].
The proficient, adroitly straightforward, semantically secure and ideally reasonable open key Somewhat FE (SHE)conspires completed the whole numbers is projected. Through a littler open key of $\tilde{O}(n^4)$ and the general plan multifaceted nature of $\tilde{O}(n8)$, the plan is equipped for scrambling number plaintexts not at all like the current FHE plans that utilize bitwise encryption. Which is n^3 for the message extension is likewise nearly low.

The security of the recommendation depends on the two-component PAGCD issue. The mathematical model of unpredictability of the recommendation is altogether investigated by contrasting and the current plans. The strategy for holomorphic encryption projected in present work sorts the encoded information preparing up and coming for all intents and purposes for reasonable applications [14]. An effective, reasonably basic, semantically secure and ideally functional open key SHE plot over the whole numbers is recommended. With a littler open key of $\tilde{O}(n4)$ and the general plan multifaceted nature of $\tilde{O}(n8)$, the plan is equipped for scrambling whole number plaintexts not at all like the current FHE plans that utilize bit by bit encryption. The missive extension is likewise relatively less, which is n^3. The information for security of the suggestion depends on the two-component PAGCD issue. The computational intricacy of the recommendation is completely investigated by contrasting and the current plans. It is normal that, the technique for holomorphic encryption is presented and same is encoded information preparing unavoidable for all intents and purposes for appropriate applications [15,16].

In [17] holomorphic encryption plot on whole number vectors, as a characteristic expansion of the as of late created holomorphic encryption system is dependent on the knowledge with mistakes presumption. As opposed to past work, concentrated on another situation, it has extensive presentations in information mists and detecting frameworks. We showed that, in this situation, the encryption plan bolsters three kinds of major tasks on whole number vectors, and dependent on which we can figure a self-assertive polynomial on whole numbers inside a specific degree productively and secretly. Likewise, we portrayed a couple of instances of calculation assignments, including highlight extraction, acknowledgment, order, and information accumulation. A solid ramification of this paper is that in spite of the fact that it is hard to build all inclusive holomorphic-encryption plans for general calculations by and by, for some particular applications we may discover straightforward holomorphic-encryption plans with sensible correspondence and calculation costs. The preparation of profound neural system with encoded datasets of holomorphic encryption, protecting the clients' security and dodging security spillage when utilizing neural systems, by figuring the whole model with numerous parameters. In our examinations reliant on MNIST, we achieve 89.05% getting ready precision with encoded dataset. Our arrangement relies upon dataset of holomorphic encryption, and after encryption we utilize mixed dataset to set up our neural framework model. Since our technique applies cryptography into significant learning, it might be acclimated to various diverse datasets before using them to continue.

At the point when direct information encryption, others can't comprehend information without mystery key, and consequently it can secure protection and guarantee clients to utilize the neural system securely [18].In [19-20], we improve Gentry's holomorphic encryption to recommend an effective, disentangled mystery key holomorphic encryption. It in the picture encryption, with the goal that the picture can be prepared in encoded structure to secure the protection. Several pictures handling that comprises of expansion and augmentation tasks on single pixel can be converted into the encoded shaped procedure. It give the shading change, picture expansion, and picture topping as the precedents. By utilizing our plan, the picture can be prepared in the server in encoded structure; after decoding in customer, client can get the right handled picture that is equivalent to handling the plain picture. So our plan can ensure protection in online picture preparing. Our plan is secure, however it expands the consecutively time of procedure and the space for putting away scrambled picture. So our plan isn't appropriate for handling enormous size of picture yet. There is a developing enthusiasm for applying AI calculation to private information, for example, restorative information, genomic information, money related information, and the sky is the limit from there. For basic applications holomorphic encryption can ensure the most elevated amount of information protection amid calculation, however it likewise accompanies a mind-boggling expense, particularly as far as calculation time [21].

Going for the issue of low proficiency brought about by excessively visit cipher text refreshing in FHE plan to accomplish a advanced productivity. It use cipher-text network activities in GSW and vectors of cipher text to increases to build security system. Moreover, consolidate the benefit of proficient holomorphic activity with the upside of reasonable development of cipher-text clamor size in GSW. In [22] for efficient and simplicity encryption process, the both matric based cipher text and vector based additions cipher texts are combined. These both will uses GSW and DM which are based NAND, AND , NOT operations and finally achieved an error less encryption [22]. In[23] paper, presented an investigated the patterns hidden advances in HE improvement, concentrating especially on enormous information. We contend that, with adequate speculation, HE will end up being a down to earth device for secure preparing of enormous informational indexes. The present patterns in the utilization of holomorphic encryption to verify huge information investigation features the developing enthusiasm for the selection of HE. This pattern is likewise supplemented by re look in upgrading the exhibition of HE through novel equipment based methodologies. The different equipment based methodologies demonstrates the developing examination movement around there. What's more, the patterns in the improvement of HE collections show that collections can be custom fitted to statement explicit huge information investigation. Later on, we will play out a far reaching overview of HE libraries and equipment based improvements to assess their presentation.

In [24] paper, we investigated attainable answers for accomplishing low-intricacy NTT-based duplication of huge whole numbers for FHE, concentrating on the equipment execution. To begin with, we have proposed a methodical method for diminishing the quantity of operands mandatory for doing the radix-r butterfly calculation, a fundamental activity in FFT/NTT applications. Methods for adequately taking care of the memory assets and illuminating the memory access clashes have likewise been introduced for further zone decrease. Our advancement has along these lines given a more reasonable arrangement than associated progress for applications, for example, FHE, which requests low-multifaceted nature and rapid enormous whole number augmentation. Recommender frameworks have turned into a significant device for personalization of online administrations.

Creating proposals in online administrations relies upon security touchy information gathered from the clients. This makes a genuine protection chance for the clients. In this paper, we intend to ensure the private information against the specialist organization while saving the usefulness of the framework.

We propose scrambling private information and preparing them under encryption to create proposals. By presenting a semitrusted outsider and utilizing information pressing, we develop a profoundly proficient framework that does not require the dynamic cooperation of the client. We likewise present an examination convention, which is the first as far as we could possibly know, that looks at different qualities that are stuffed in one encryption. Directed tests demonstrate that this work opens a way to create private proposals in a protection safeguarding way [25].In [26] begun with three issues: Zero's assault, concealing relations among records and saving recovery reasonability. We proposed a structure that regulates the TF-IDF tables; this framework conceals the colossal number of zeros (or any exceedingly frequented attributes) in the tables comparatively as some other relationship between records since it keeps the zeros. The strategy was related on three different datasets; results demonstrate that the system improves the recovery sufficiency even with little qualities. The going with stage is to discover a system to recover just the picked archives without giving any data about them to both the customer and the cloud, or by righteousness of sending the similarity vector to the customer, she won't doubtlessly know anything about the un chosen reports, the technique ought to additionally shield the cloud from evaluating any relationship between the record records and the past solicitation on the proportionate dataset; this approach should combine with the recommended structure in this paper to fulfill the necessities of a "Security Preserving Search in Data Clouds". Modernized watermarking is a system that presents impelled data inside a transport signal. Beginning late, Watermarking has been a working territory of research. These watermarks can be utilized to check the legitimacy or respectability of the transporter signal or can be utilized to display the character of its proprietor. The photographs can be verified in cloud based stores. Here the security must be considered. In this way, the picture is blended utilizing holomorphic encryption plot and can be gotten to by expected people by unscrambling it utilizing holomorphic unwinding plan. Before long, Homomorphic cryptosystem has been generally utilized any place all through the open cloud. In homomorphic cryptosystem, the client can perform practices on the blended information without unraveling the information and get a tantamount outcome as performed on the fundamental information. Along these lines, it keeps up riddle over the cloud based stockpiles [27].

II. PRELIMINARIES OF FHE, SHE AND DGHV SCHEMES

In the communications, the main parameter to be considered is security with minimal computational operations and lessor delay. Most of the security algorithm like AES, ECC and Reed Solomon systems are required larger key size for more security, out of which AES is widely used and having more security therefore, in this research work AES-128bits of 10 round operations is proposed as second part of this work, the first part of this work is acquiring an ECG/EEG and Image from sensors and then converted into integer values as plain text and key. The conversion of the signals into integer as follows, let P and Q are the integers in DGHV, the quotient of the division P/Q is represented as X_p (P/Q) and assume Y represents adjacent integer which can be unique, the division remainder represents R_p (P/Q). Finally, the modulo process of X_pw.r.t$R_p$is $|M|_p$ or $X_p$mod $R_p$thus R_p (P/Q)=$|M|_p$-X_p (P/Q).P.

When P is an odd integer then $\mathrm{Rp}\ (X) \in (\frac{-P}{2}, \frac{P}{2})$

The encryption of the FHE for the given plaintext is defined as

$$y \leftarrow a + 2p + 2\sum_{j=1}^{\tau} q_i . b_i mod\, q_0$$

Where a∈ {0,1} is the information signals bits, p is the randomly generated noise, $q_i$is the integer which converted from EEG/ECG signals as plaintext or key, b_i is the selected randomly generated key.

The SHE operates for any polynomial i.eP $P = \frac{A[x]}{B_m(x)}$, the both plaintext and key can be polynomial.

III. METHODOLOGY

3.1 Proposed Holomorphic encryption using AES algorithm

The proposed holomorphic is taylor analytical function having complex analysis in terms of infinitely differentiable, locally and equal. Let AB represents the closed complex unit for the disk and f:A→X, f:B→Y be conditions function then assume to be approximate ff by using holomorphic function hh in the uniform metric and search to find the minimize sup{X∈A:|g(X)−f(X)|}sup{X∈A:|g(X)−f(X)|} subjected to the condition that hh be proposed holomorphic of the disk of the interior. As discussed in previous section about SHE, FHE and DGHV that has only two variable for encryption of the data but in case of the holomorphic has three more variables such as plaintext integer(PI) to be encrypted using AES, secrete key integer(KI), and multiple of which is the public key integer (PKI) with additive error. For allowing of the maximum number plaintext's over holomorphic encryption takes as ≥PI.Ø(mlog2 m), where m is information integer values in the plaintext, Ø is error function in holomorphic function. The constraint e is the bit length of the mystery key number P. To help homomorphism on behalf of adequately more profound designs, e is reserved as ≥e'.ø(m(log(g)^2 m) variable g is the quantity of bits in every one inpublic key whole numbers. All the more exactly, Q factor of the length of the bit to acquire the products of P in the open key. Subsequently the open key comprises of just two components, the assaults identified with the two-component PAGCD issue just are considered. In perspective on same, it is adequate toward fulfill the g > e condition.

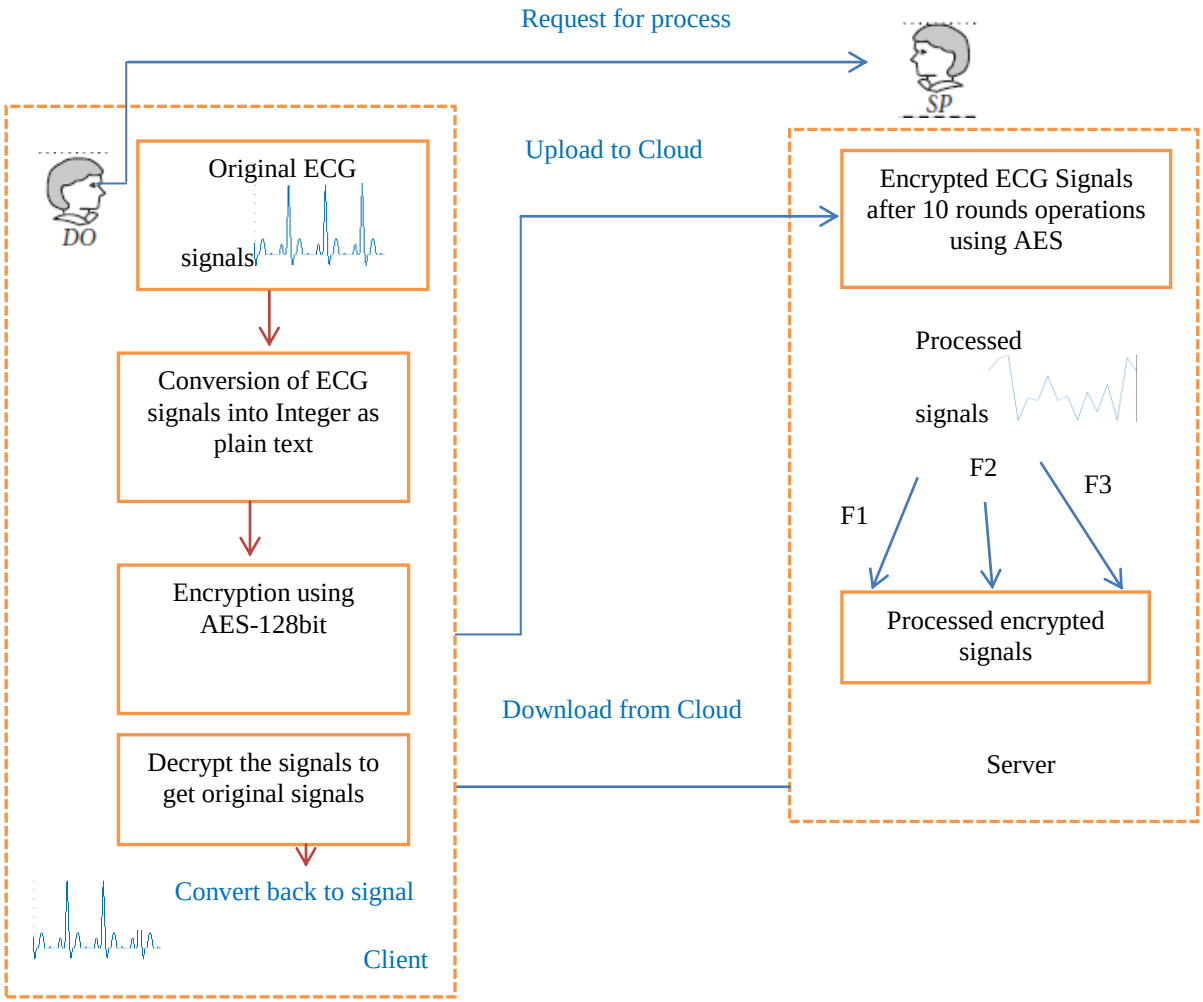

Fig.1. Proposed block diagram of integer encryption and decryption using Holomorphic and AES algorithms along with cloud interface.

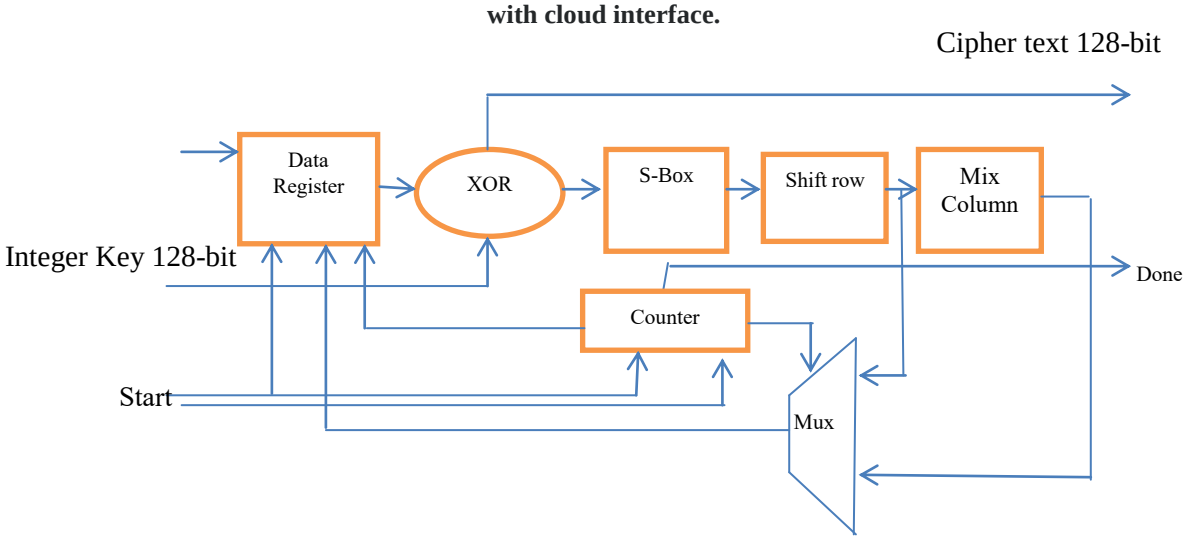

Fig.2. Proposed Encryption process using AES

The proposed secrete key holomorphic encryption algorithm over bigger message space, consequently indicated as HL, the complete explanation with example is describes in the following two examples.

Example:1 Secrete key for encryption HL=(inputs and outputs)={key, enc,dec, evaluate) and these are algebraically holomorphic for the EEG/ECG which are converted into integers for the given plaintext $P \in Z \cap [-2^{p-1}, 2^{p-1}]$ and any key integer $KI \in KI_p$.

Algorithm for example:1

Inputs: Plaintext and Secrete Key:P_1 and SK_1

Outputs: Cipher text :CT

Step:1

$X_2=[P_1,SK_1]$mod

$X_0=P_1.(QQ'+PQ_1) \bmod X=QQ'+PP_1Q_1-T_1PQ_0$ for any integer values ofT_1

$$=QQ'P_1 + P(P_1Q_1 - K_1Q_0) = QQ'P_1 + PQ'$$

CT=[outputs]=

$$[Y + Y_2.X_2] mod\ X_0 = Y + N_2(QQ'P_1 + PQ^i\})] mod\ P_1 = Y + QQ'P_1 + P(Y_2Q^1)] mod$$

$X_0$for the integer K_2

=Y+QP_1+PQ for the given integer P and Q. The output of the CT is a nearly to numerous of integer P.

Maximum value of plaintext P_1 is subjected to encryption is 2^{p_1-1} and to get back the original data is usually called cipher text and using it decryption is Y+QN should be less than original plaintext or key size.After the example 1 process completes then the output is subjected to AES encryption which involves add around block, shift row, Substitution-Box, Mixture Column and add around key as shown in the Fig.2.

In like manner the proposed work offers the favored position in zone. In like way in the proposed work the bits are fixed up on information course from register to S-Box and the round persistent required for each round are verified in ROM and recovered on each clock. Fig.2 addresses proposed structure of key age unit. Begin, stop_mix, end are control sign made by the control unit. The "done' signal is given to display that encryption is done arrangement is as appeared in Fig. 3. In the proposed work for decreasing the equipment of whole structuring, the control unit of encryption module isn't composed unreservedly. The control unit of key age module which is a 4-bit counter is wanted to control the whole working of encryption module. The sharing of control unit by both encryption and round key age gives remarkable perfect position of reducing in equipment when emerged from different executions and its stream visit is showed up in Fig.3.

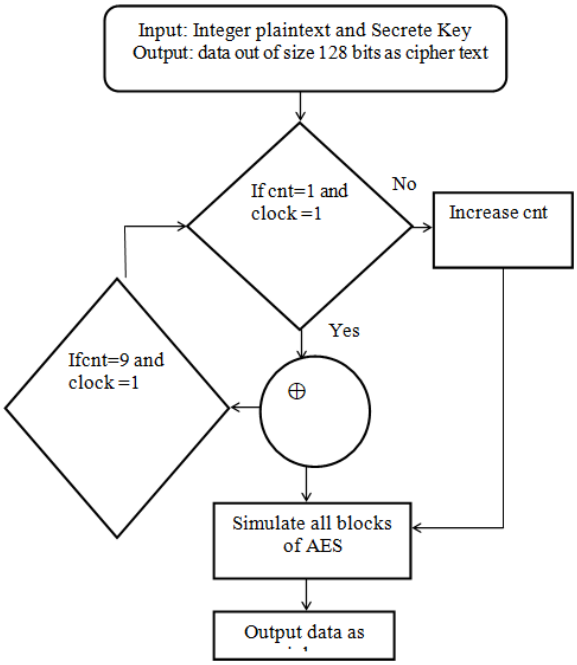

Fig.3. Flow Chart of AES for integer input values

Example: 2

Consider with an example for numerical value and corresponding secrete parameter m=4 and holomorphic it is convenience in calculation for the value k=m instead of 3m as specified in the holomorphic scheme.

Secrete Key Generation: Let P= 17063439657879604805, 128 bits R = 60071, 16 bits. Then the secrete key SK=(P,R). Generated secrete key of 128 bits random integers, Q0 = 97664186810858587266931265562377884310814380857833474263451469838559278518704, and Q1 = 82721281349971397170778552573254573840245659574711407902336764309256718858076. Select a 4-bit arbitrary integer R' = 11. Calculate, X0 = PQ0 = 16664869583829666641847990410257817571623068345609838267147170219901875295756713655069133207727 20, and X1 = PQ1+RR' =14115095927377184708507520831075117132566624078473597764733467379628436973711684890060297633159 61. Public key PK = (X0, X1). This results are as per below results

```
N1=3;
R1=randi(15,1,1);
X0 = P*Q0;
X1 = ((P*Q1)+(R*R1));
X2= mod((N1*X1),X1);
N2=randi(15,1,1);
C1(1,i) = mod((M(1,i)+(N2*X2)),X0);
```

The encrypted integer data is ready now to upload into cloud and store the data in https://thingspeak.com/ by creating an account in it. The each packet is of 128 bits and it will take 15 sec to upload into cloud as shown in Fig.4.

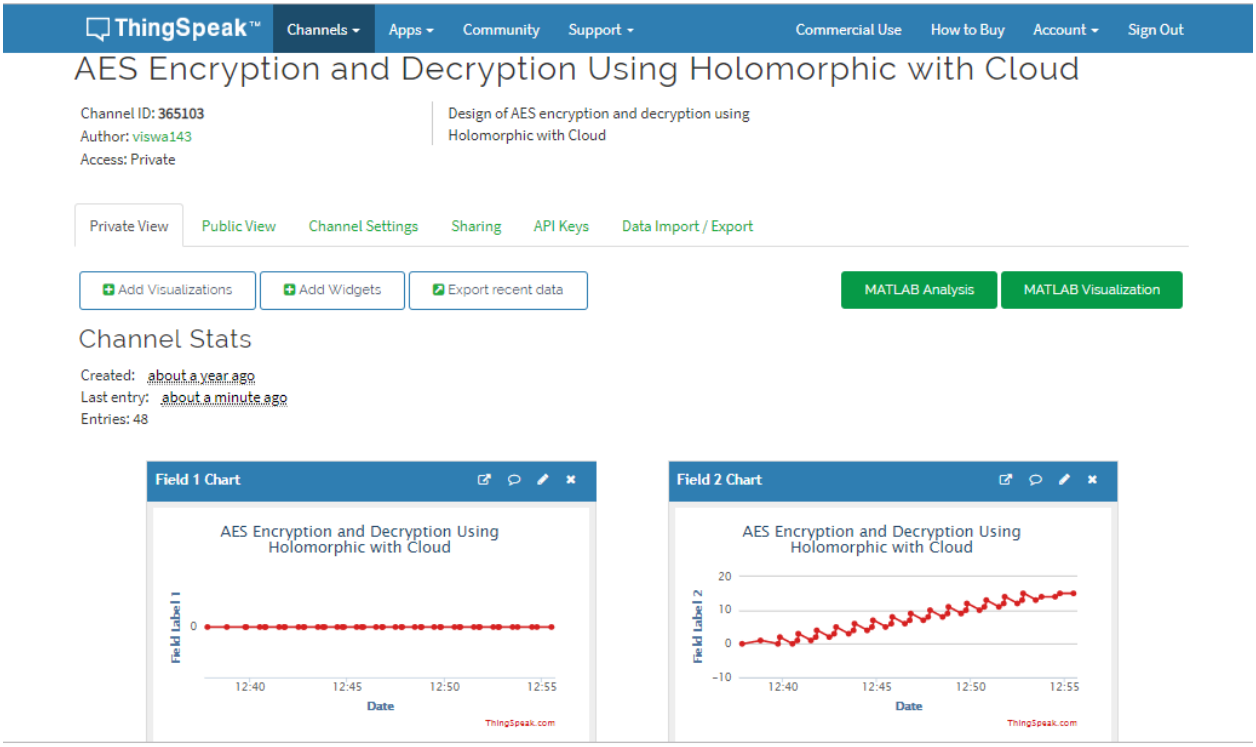

Fig.4. Interfacing with Cloud for storage of cipher text and integer secrete key

IV. DOWNLOAD THE DATA FROM CLOUD:

The proposed research work is successfully verified by uploading the packets into cloud in ThingSpeak. To interface with cloud there are three variables are used such as Channel ID, API keys called Write key and Read key, the write key is for storing the packets in the cloud as shown in Fig.4 and Read Key to read the packet from the cloud to MATLAB environments. Each packet takes 15sec for writing and to read into cloud and read from cloud. The IoT frameworks may contain latent also, dynamic hubs. This implies the interactive media information may be transmitted through vitality based hubs or typical hubs. Concerning ordinary hubs, the vitality isn't an essential factor. For the vitality based hubs, IoT-RTP ought to know of the condition of these kinds of hubs. In this manner, a field ought to be included the IoT-RTP to record the vitality level for each hub in the interactive media session.

Proposed algorithm: Combined IoT-RTP and RTCP-IoT

U is the number nodes (users) used as multimedia metadata in the session i.e 4 those are EEG, ECG, Audio signals and Polypoid WCE images having symptoms disease

P: Number of sub-sessions

Q: Sub-Sub sessions numbers

C: Network Capacity in all the sessions

C_{div}: Capacity of the network after the dividion of sub sessions

F: Number of the sub-flows

$$if \sum_{j=1}^{U} session\ Id \leq C)$$

Stay in the initial stage

else

for X=1 to P

begin

$$if \sum_{j=1}^{U/P} session\ Id \leq C_{div})$$

Stay in the initial stage

else

$$pf_i = \frac{session\ id}{F}$$

$$if \sum_{j=1}^{U/P} session\ Id \leq C_{div})$$

Stay in the initial stage

else

for i=1 to 4

pf_i should be transmitted through RTP and upload to cloud for storage though (thingspeak.com)

end

Termination of the algorithm

IoT RTCP

The flexible variation of RTCP in like manner deliberates the state of the IoT structure regarding the transmission of blended media streams. In like manner, its intelligences assemble information aroundpossessions that may be originating in the IoT structures and that shift from various schemes. It may variation moreover thinks about the kind of center points (dynamic or idle).

The specs of everything in the IoT structure, for instance, dealing with, memory and imperativeness, should be considered. Moreover, unprecedented blended media coding must be reflected. Minimization of RTCP intelligences without impacting the sight and sound communicationcomplete IoT structures is a fundamental concentration in RTCP,

especially if there ought to be an event of framework famishment. To accomplish the goals, prioritization of control reports should be associated. In the standard RTCP, there are two essential sorts of reports, specifically sender report (SR) and beneficiary report (RR). SR contains various elements, for instance, the amount of transmitted packages inside a period, the various fields of the RTCP such as Network Time Protocol (NTP), and synchronization sources, timestamps. In RR field contains various fields, for instance, divide lost (FL), assessed number of groups expected (NPE), and between landing jitter. In SR, RR and RTCPmust be refreshed by accumulation various fields to collect express dataaround the IoT structure. In like manner, these intelligenceswill be communicated under kept surroundings so as to confine the over-troubling of the additional fields. As communicated above in the major idea of IoT-RTP, IoT-RTCP furthermore isolates the intelligent media session into a get-together of clear sessions. All sessions has a chairman that is picked using the framework uncovered. The division of blended media session methods should be constrained with session measure [1]. In case the sight and sound session measure is greater than a destined edge, In any case, by virtue of a standard sight and sound session, the division system will be overlooked. The edge what's progressively, normal sizes are depicted in the reenactment fragment.

Proposed algorithm: RTCP-IoT with Cloud storage

AT: Allocated time for receiving of the packet in the interval on the reception of the report (RR).
UL: Upper level of complete multimedia divisions.
ML:After Separation of the Middle level sessions.
NL: After Separation of the Lower level of session.
EED:end-end-delay.
PL:packet loss.
J:Jitter with delay
R:Report on the reception of the packet
$if(TP < AT)$
begin
for K=1 to UL
begin
for Z=1 to M
begin
for Q=1 to N
begin
if(EED, PL, J are standard logics)
begin
IoT-RTCP
stopped the additional fields
Report on the reception of the packet
$R_K = R_Z + R_Q$
end
else
begin
AT value should be increased and include additional fields for the RTCP and send $R_K = R_Z + R_Q$
end
$R_M = R_{UL} + R_Z$
end
$R_{UL} = R_Z + R_M$then receive the packets from the cloud and plots in the MATLAB for validations of multimedia datasets
end for termination

1. ALGORITHM/ PROPOSED METHODOLOGY

The proposed methodology/ algorithm can be broadly classified into following:
Step 1: select the patient for analysis
Step 2: read the input data from the various sensors inserted to patient.
Step 3: By receving the data from different sensors by creating wireless body area network.
Step4: start transmitting data using RTP/RTCP.
Step 5: analyse the data for uploadin to cloud
Step 6: receive data through cloud storage using same protocol during transmission.
Step 7:e-health monitoring system for assisting the data share to expert.
Step8: remote access by the doctor
Step9: generate the respective prescription for particular patient
Step 10: repeat step4 to step 6
Step 11: the corresponding prescription will reach through safe and efficient channel to
patient care taker.

V. RESULT AND DISCUSSION

In this paper, we have demonstrated to use integer data of the EEG/ECG data which is captured using wireless capsule signals are processed using AES for encryption and decryption through protocols RTP and RTCP protocol. As our application in the consideration is the data processing using the wavelet and uploading onto cloud storage. The sample outputs are as shown below in figure

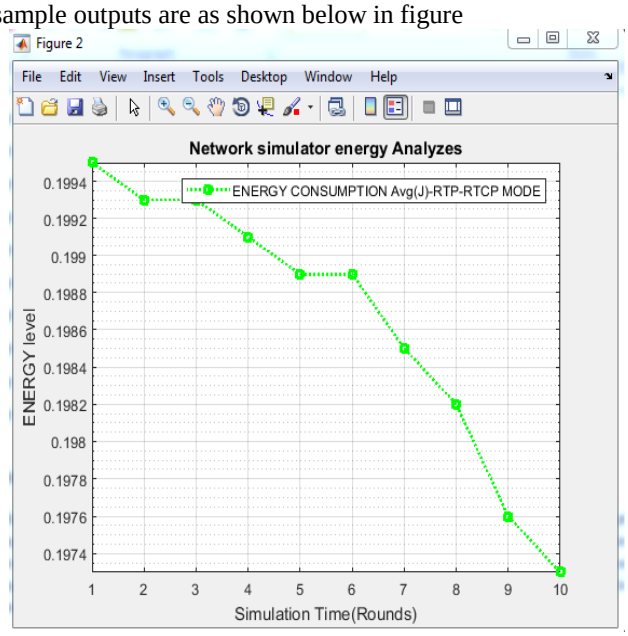

Fig.5 (a). Packet uploaded into cloud and their energy consumption and packet delivery ration

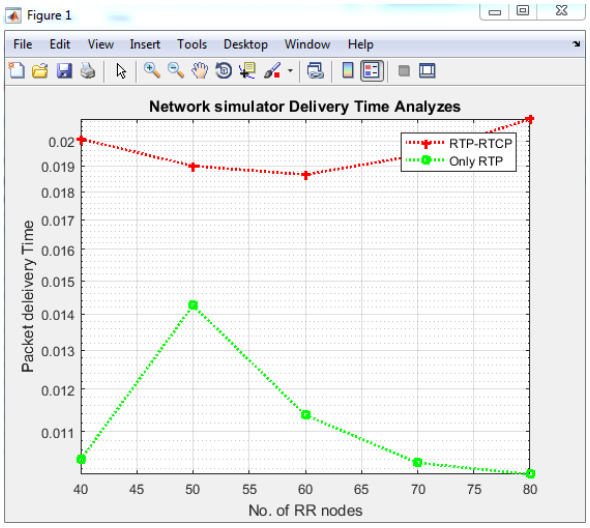

Fig.5 (b). Packet uploaded into cloud and packet delivery ration

VI. VALIDATION OF THE SECURITY LEVEL FOR THE PROPOSED SCHEMES

The level security of the proposed Holomorphic encryption algorithm, AES-128 bit, RTP-RTCP and Cloud interfacing is validated by considering security parameter n and odd integer positive random numbers of public elements (Y_o,Y_1). Let (A,B) is the secrete key and (Y_o,Y_1) public keys. Each key of Secrete key is mapped and multiple with A and other key is mapped and multiple to B. The ciphertexts created by the plan are likewise inexact products of P, however, with a high clamor or added substance mistake when contrasted with that of X1.In this manner, the pair of public key components is the littlest conceivable occasion to fathom the PAGCD issue. Any non-immaterial favorable position in speculating the equality of the plaintext whole number in an arbitrary ciphertext that contains high clamor can be changed over in to the capacity to take care of the two component PAGCD issue utilizing the pair of open key components (Y0, Y1) containing low commotion.Because of the likenesses in the development and type of ciphertexts, the proposed HEL and the DGHV plan are indistinguishable with just contrasts in the plaintexts they encode what's more, the open key size. Henceforth, a similar system utilized in [4] and CMNT plot [8] can be connected in decreasing the security of the plan HEL to taking care of the two-component PAGCD issue.

VII. CONCLUSION

In this research work, the design is successfully simulated in MATLAB 2017a by installing IoT and ThingSpeack packages. By using Holomorphic encryption algorithm, the EEG, ECG and Images are converted into integer values. The EEG and ECG signals are acquired for the duration of 10ms which contains 1000 samples/coefficients, therefore after converted into integer values, there are totally 1000 values, whose values formatted 16 integer values as one packet to upload into cloud through RTP-RTCP protocol. An effective, theoretically simple, semantically provides the security and ideally commonsense open key SHE plot over the whole numbers is projected. With a littler open key of $\tilde{O}(n^4)$ and the general plan unpredictability of $\tilde{O}(n^8)$, the plan is equipped for scrambling number plaintexts dissimilar to the current FHE plans that utilize bitwise encryption and same is encrypted using AES-128bits. The message extension is likewise nearly low, i.e n^3. The semantic security of the suggestion depends on the two-component issue of PAGCD. The computational intricacy of the recommendation is altogether broke down by contrasting and the current plans. It is normal that, the strategy for holomorphic encryption proposed in this work makes the scrambled information preparing approaching for all intents and purposes for reasonable applications.

REFERENCES

1. C. Gentry, “A fully homomorphic encryption scheme”, Ph.D Thesis, Stanford University, 2009
2. C. Gentry, “Fully homomorphic encryption using ideal lattices”, In STOC, pp 169-178, ACM, 2009.
3. N. P. Smart, F. Vercauteren, “Fully homomorphic encryption with relatively small key and ciphertext sizes” In Public Key Cryptography - PKC'10, Vol. 6056 of LNCS, pp. 420-443,Springer, 2010
4. M. V. Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan, “Fully homomorphic encryption over the integers”, Proceedings of Eurocrypt,
5. Vol. 6110 of LNCS, pp. 24-43, Springer, 2010.
6. C. Gentry, “Computing arbitrary functions of encrypted data”, Communications of the ACM, 53(3), pp.97-105, 2010.
7. D. Stehlé, R. Steinfeld, “Faster fully homomorphic encryption. ASIACRYPT’2010, Vol. 6477 of LNCS, pp.377-394, Springer, 2010
8. N. Ogura, G. Yamamoto, T. Kobayashi, S. Uchiyama, “An improvement of key generation algorithm for Gentry’s homomorphic
9. encryption scheme”, Advances in Information and Computer Security - IWSEC 2010, Vol. 6434 of LNCS, pp. 70–83, Springer, 2010.
10. J. S. Coron, A. Mandal, D. Naccache and M. Tibouchi, “Fully homomorphic encryption over the integers with shorter public keys”, CRYPTO 2011, P. Rogaway (Ed.), Vol. 6841 of LNCS, pp. 487-504, Springer, 2011.
11. Z. Brakerski, V. Vaikuntanathan, “Efficient fully homomorphic encryption from (standard) LWE”, Electronic Colloquium on Computational Complexity (ECCC) 18: 109, 2011.
12. Z. Brakerski, V. Vaikuntanathan, “Fully homomorphic encryption from ring-LWE and security for key dependent messages. CRYPTO 2011, pp.505-524.
13. Z. Brakerski, C Gentry, V. Vaikuntanathan, “Fully homomorphic encryption without bootstrapping”, Electronic Colloquium on Computational Complexity (ECCC) 18: 111, 2011.
14. P. Scholl, N.P. Smart, “Improved key generation for Gentry’s fully homomorphic encryption Scheme”, Cryptology ePrint Archive: Report 2011/471, http://eprint.iacr.org/2011/471
15. Y Govinda Ramaiah.et.al, "Efficient Public key Homomorphic Encryption Over Integer Plaintexts", 978-1-4673-2588-2/12, 2012 IEEE.
16. Naveen Ghorpade.et.al, "Towards Achieving Efficient and Secure way to Share the Data", 2017 IEEE 7th International Advance Computing Conference, 978-1-5090-1560-3/17, 2017 IEEE, DOI 10.1109/IACC.2017.10.
17. Hongchao Zhou.et.al, "Efficient Homomorphic Encryption on Integer Vectors and Its Applications", This work was supported in part by Draper Laboratory through the UR&D Program and by AFOSR under Grant No. FA9550-11-1-0183.
18. Tianying Xie.et.al, "Efficient Integer Vector Homomorphic Encryption Using Deep Learning for Neural Networks",Springer Nature Switzerland AG 2018, L. Cheng et al. (Eds.): ICONIP 2018, LNCS 11301, pp. 83–95, 2018. https://doi.org/10.1007/978-3-030-04167-0_8.
19. Pramod Kumar Siddharth,et.al, "A Homomorphic Encryption Scheme Over Integers Based on Carmichael’s Theorem",2016 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT),978-1-5090-4697-3/16,2016 IEEE.
20. Pan Yang.et.al, "An Efficient Secret Key Homomorphic Encryption Used in Image Processing Service",Hindawi Security and Communication Networks Volume 2017, Article ID 7695751, 11 pages https://doi.org/10.1155/2017/7695751.

21. Hao Chen.et.al, "Logistic regression over encrypted data from fully homomorphicencryption",BMC Medical Genomics 2018, 11(Suppl 4):81, 10.1186/s12920-018-0397-z.
22. XunWang, et.al, "A More Efficient Fully Homomorphic Encryption Scheme Based on GSW and DM Schemes", Hindawi Security and Communication Networks Volume 2018, Article ID 8706940, 14 pages https://doi.org/10.1155/2018/8706940.
23. Roger A. Hallman.et.al, "Homomorphic Encryption for Secure Computation on Big Data",In Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018), pages 340-347, ISBN: 978-989-758-296-7, 2018 by SCITEPRESS – Science and Technology Publications.
24. Jheng-Hao.et.al, "Low-Complexity VLSI Design of Large Integer Multipliers for Fully Homomorphic Encryption", IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 26, NO. 9, SEPTEMBER 2018, 1063-8210,2018 IEEE.
25. Zekeriya Erkin.et.al, "Generating Private Recommendations Efficiently Using Homomorphic Encryption and Data Packing", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 3, JUNE 2012, 1556-6013, 2012 IEEE.
26. Mohanad Dawoud.et.al, "Privacy-Preserving Search in Data Clouds Using Normalized HomomorphicEncryption",Euro-Par 2014 Workshops, Part II, LNCS 8806, pp. 62–72, 2014.Springer International Publishing Switzerland 2014.
27. G. Dinesh Kumar.et.al,An Efficient Watermarking Technique for Biometric Images", Procedia Computer Science 115 (2017) 423–430, 1877-0509, 2017 Published by Elsevier B.V.