International Journal of Intelligent Networks 3 (2022) 16–30

Contents lists available at ScienceDirect

International Journal of Intelligent Networks

journal homepage: www.keaipublishing.com/en/journals/international-journal-of-intelligent-networks

A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing

Fursan Thabit [a,*], Ozgu Can [b], Sharaf Alhomdy [c], Ghaleb H. Al-Gaphari [c], Sudhir Jagtap [d,**]

[a] Postdoctoral Researcher, Department of Computer Engineering, Faculty of Engineering Ege University, Turkey
[b] Assoc. Prof Dr., Department of Computer Engineering, Faculty of Engineering Ege University, Turkey
[c] Professor Faculty of Computer and Information Technology (F.C.I.T.), Sana'a University, Yemen
[d] Professor and Principal, Research Centre of Computer Science, S.V.M Campus - S.R.T.M. University, India

ARTICLE INFO

Keywords:
Cloud computing
Light-weight cryptographic
Multiplicative homomorphic
RSA
cloud base IoT

ABSTRACT

Cloud computing is a technology in which the resources are delivered as services. Users can access them anywhere, anytime via the Internet without any need to know the infrastructure knowledge, experience, or even authority that provides such services. It has become an important medium for enterprises to develop their networks because of these resources. With the growing need for cloud computing, security is becoming important for both individuals and business needs. Many researchers have studied the security of cloud computing. Still, security gaps or threats are increasing as the demand for cloud computing connectivity increases. Because a third party mostly provides cloud platforms to the cloud client, data protection in the cloud is the primary issue. This paper presents a novel, effective lightweight homomorphic cryptographic algorithm which contains two layers of encryption. The first layer uses the new effective, light-weight cryptographic algorithm and the second layer multiplicative homomorphic schemes considered for improving security data in cloud computing. This approach offers both symmetric and asymmetric cryptography features. The proposed approach's performance is evaluated using a variety of metrics, including memory, computational time and (key sensitivity), statistical analysis, image histogram, and entropy change analysis. The proposed algorithm's experimental findings showed a high level of security and an apparent improvement in encryption execution time, memory usage, and throughput. When compared to the cryptographic systems widely used in cloud computing.

1. Introduction

In the past few decades, communication has been developing rapidly among users via the Internet. In addition, data usage has been increasingly growing among a variety of users. Transmission of valuable and confidential information has been at a higher level. Security of confidential information is a must for secure transformation. One of the areas for storing confidential information is the cloud, and data security in the cloud is one of the issues that must be addressed.

Cloud computing is a trend in the field of information current technologies. Therefore, many business applications require new innovations to be applied to store or process big data. Cloud computing is a cutting-edge method of storing large amounts of data and running applications [1]. It allows users to have nearly infinite processing capacity and offers possible advantages in terms of easy accessibility, scalability, and resource sharing. The cloud services involve online file storage, webmail, social networking platforms, and online business applications. On-demand self-support, comprehensive network connectivity, resource pooling, rapid flexibility, and controlled application are all essential functions of cloud computing. Clients (people or organizations) can order and control their machine services via on-demand self-service. The distribution of services across the Internet or private networks is made possible by access to pooled resources. Cluster services mean that clients are derived from various computing resources, typically in remote data centers. Rapid versatility ensures that programs can be changed more or less. Product utilization is assessed, and consumers are billed accordingly [2]. Cloud storage has become an advanced model of service, the usage of its technologies by users (businesses, individuals, etc.) are restricted due to concerns over the lack of privacy of their private data.

Based on the rate of cybercrime on the Internet continues to rise.

* Corresponding author. Department of Computer Engineering, Faculty of Engineering - Ege University Turkey.
** Corresponding author.
E-mail address: thabitfursan@gmail.com (F. Thabit).

https://doi.org/10.1016/j.ijin.2022.04.001
Received 28 July 2021; Received in revised form 11 April 2022; Accepted 12 April 2022
Available online 16 April 2022

Cloud computing has become a magical target for many reasons.

In order to protect all of the services and benefits offered by cloud computing and the Internet, data security is essential. Data confidentiality can be achieved across the network using encryption technology, which is encryption and decryption. Cryptography aims to provide a security function bundle that can ensure the confidentiality of the system. These objectives can be categorized into the five categories listed below [3].

- Authentication: The identity of the sender and recipient must be verified before sending the message.
- Confidentiality: Only authorized users can interpret the message, and no one else can use it.
- Integrity: ensuring that the content of the transmitted data does not contain any kind of modification.
- Service reliability and availability: As intruders influence service availability to users. The technology should provide users with the service quality they expect [4].
- Non-repudiation: This function indicates that neither the sender nor the recipient can deny that a particular message has been sent.

Cloud security is one of the most difficult and promising computer technologies which provide various communications to the user. In other words, cloud data security is another advancing pattern in data innovation where more security for data is essential. Traditionally, the data centers maintain and control the data but are insecure. They are prone to various types of attacks. Hence, there must be an effective mechanism for providing secure transformation and privacy-preserving of data in the servers. An immense amount of information is shared over the system by utilizing the various services and lots of information is stored in the cloud server. Various schemes of encryption were adopted for protecting and securing the information in the cloud.

Cryptography is considered to be one of the safety measures for secure communications. To bridge the security gap, the most widely used technique is the encryption of remotely stored data. The cloud environment keeps on changing rapidly, and this poses a fundamental challenge for outsourcing computation. Hence, it has created an impetus for many computing researchers to improve available symmetry/asymmetry algorithms [5–9].

The encryption and decryption technologies are available in three types: symmetric, asymmetric, hybrid algorithms which may be utilized in cloud storage to encrypt and decode data [10].

Symmetric encryption is a cryptographic technique in which the sender and recipient share a single public key to encrypt and decrypt the data. The standard symmetric algorithm used for data cryptography is the Data Encryption Standard (D.E.S.), the Advanced Encryption Standard (A.E.S.) [11].

Asymmetric encryption consists of two distinct keys: the encryption used the public key and decryption used the private key only the authorized receiver able to decode the message using the private key. An asymmetrical algorithm example used for data cryptography is the R.S.A. algorithm.

Hybrid encryption is a kind of encryption that integrates multiple or more encryption algorithms, using a combination of symmetric and asymmetric encryption to take use of each type's capabilities. This hybrid cryptography method was created in order to provide an efficient and secure encryption algorithm capable of encrypting and decrypting data fast and safely [12]. Since the advent of the Data Encryption Standard (DES), lightweight block ciphers have played an increasing role in cryptology.

Many lightweight architecture is designed for both VLSI and resource constrained environments. Most of them used chaotic map, cellular automata and genetic algorithms in AES and elliptic curve for randomization. Lightweight block ciphers are commonly implemented to provide bulk data encryption and are important building blocks in the construction of many cryptographic protocols.

According to the related work, present encryption techniques and the design of cryptographic processes offer both advantages and disadvantages.

- Existing techniques use the same type of generator to generate keys.
- The same key is used for all data types.
- There is no pattern randomization for message encryption.
- Information is freely accessible to third-party users.
- Patterns must be manually updated.

To address all of these issues, this article work aim to design a new Lightweight Homomorphic Cryptographic Technique for enhanced the security in cloud by using the random pattern generation for key and S-box.

In this article, we propose an effective solution that aims to enhance the security measures in the cloud. The article presents a Novel, Effective Lightweight Homomorphic Cryptographic Technique, which contains two layers of encryption. The first layer uses the new effective, lightweight cryptographic algorithm and the second layer applies multiplicative homomorphic schemes for improving security data in cloud computing. This technique's offers both symmetric and asymmetric cryptography features. The proposed technique's performance is evaluated using a variety of metrics, including computational time, memory, (key sensitivity), statistical analysis, and entropy change analysis with image histogram. The significant contributions can be described as follows:

1) A novel 128-bit Lightweight cryptography technique based on substitution permutation (SP) and Feistal and architectural methods with theory of diffusion and confusion of Shannon's through the use of logical operations, such as (XNOR, XOR, shifting, swapping) to improve the complexity of the encryption which use in the first layer of encryption.
2) A novel 128-bit secret key generation technique is based on logical operations (XOR, XNOR, shifting, swapping).
3) The Multiplicative homomorphic property of R.S.A. algorithm is introduced in the second layer of encryption
4) The experimental results of the purpose algorithm are presented to verify its efficiency on current Encryption techniques.

The following are the portions of the paper: The first section is meant to serve as an overview. The second section outlines a study that is linked to the research. Section 3 explains the suggested algorithm. The simulation and implementation environments are described in Section 4. Section 5 summarizes the findings and comments. Section 6 contains a comparative analysis. The CIA's security analysis and accomplishments are described in Section 7. Other conclusions and recommendations were being stated in Section 8.

2. Related work

Cloud computing is a transformation in computer technology. It addresses various conventional computing challenges, including managing peak loads, downloading program upgrades, and using redundant computing intervals. Cloud computing has a major impact on every aspect of our lives as well as the market structure. In a cloud computing context, data security is a major concern. Several research initiatives have been suggested to protect cloud data.

The author of [13] presented a hybrid cryptography approach for cloud security and privacy that used both symmetric and asymmetric key techniques. This technique will be used for encryption and decryption operations with key creation. Super Elliptical Curve Cryptography has been used to enhance data encryption in the cloud (HECC.). The developers of [14], created a hybrid encryption hashing method for cloud computing data storage that prevents data theft. They used hybrid algorithm RSA, AES and hash functions to protect cloud

data storage using a separate data input size (34, 67, and 93 kb).

The authors of [10] suggested a method for securing cloud computing user data using encryption techniques, they used several algorithms. They suggested a variety of algorithms to address issues related to data loss, disconnection, and privacy. They evaluated the accuracy of R.S.A., D.E.S., A.E.S., and Blowfish algorithms to data encrypt and decrypt in the cloud. The authors of [5] developed a cryptographic method to increase security data in cloud storage. According to the technique, data might be encrypted before being transmitted to the server. The confidentiality of the data provided by the customer is ensured in two ways the algorithm encrypts the data and only permits active authentication to access it. In this algorithm, the provided file will be encrypted using the A.E.S. algorithm. The A.E.S. key is encrypted using the R.S.A. algorithm. The created algorithm encrypts and stores the file in the cloud, whereas the recommended approach encrypts and stores the text in the cloud. The authors of [15] developed a methodology to increase cloud data security. They developed a simple encryption method. The methods operate in three phases. First, swap the keys. This phase is divided into two parts: key creation and key exchange. The encrypted data is saved in the cloud in the second data storage. The user's third access to data is when they request data from cloud storage.

The authors of [1] developed a symmetric approach. The procedures are implemented on a block-by-block basis. The approach encrypts up to 192-bit blocks of data into cypher text at a time. In 12 cycles, the symmetric method encrypts and decrypts the data. Because the technique applied a 192-bit key, it provided more security. In Ref. [16], studied and assessed the most essential data protection security methods that cloud computing companies have previously embraced. They divided them in four different categories based on methods of the security they offer: confidentiality, access control, and Authentication, with authorization are all aspects of information security. The author [17] provides a performance evaluation of six standard symmetric block encryption algorithms, which are D.E.S., 3DES, A.E.S., RC6, RC2 and Blowfish,. The results revealed that Blowfish outperformed other standard encryption algorithms, followed by RC6. The authors [18] present homomorphic encryption to provides better security data in multi-cloud. The algorithm improves security data, segregation, ownership and privacy. The [19] proposed a simple encryption algorithm that is completely homogeneous.

The algorithm was derived from the gentry' cryptosystem using only the standard computation. It has the potential to maintain privacy in an unreliable third-party cloud. The author [20] analyze the different applications of symmetric cryptography in particular as it applies to information privacy in the cloud. The author [21], explored real-time problem of homomorphic coding application. The study present implementation of homogeneous plots using Field Programmable Gate Arrays (FPGAs) and GPUs. This paper [6] investigates the use of several Homomorphic Encryption cryptographic algorithms (R.S.A., Paillier, ElGamal) on a Cloud Infrastructure. They are compared on four criteria: Homomorphic Encryption type, data privacy, security applied, and keys applied.

In addition, several symmetrical cryptographic algorithms for lightweight applications designed and developed, such as L Block, D.E.S. L., L.E.D. HIGHT, PRESENT, C.L.E.F.I.A., TWINE, S.I.T., RECTANGLE, and others, have been investigated and developed. "A lightweight 64-bit block size cryptographic algorithm with a 128-bit key was developed, iterated in 32 rounds, and performed two sorts of operations: XOR operations paired with left or right rotations. Its primary goal was to instal hardware on ubiquitous devices such as wireless sensor nodes and RFID tags that had the same chip size as A.E.S. but ran significantly faster." "[22].

The study in Refs. [20,23] developed the generalized multi-platform cryptosystem Feistel structure known as "TWINE." It has a block size of 64-bit and 36 rounds with either an 80-bit or 128-bit length key, with each round containing a 4-bit S-box and a 4-bit block permutation layer, as well as a non-linear replacement layer. The "RECTANGLE" cryptosystem, according to the authors of [8], is optimized for a 64 bits block size with a key length of either 80 or 128 bits and runs just 25 rounds. A stable IoT (S.I.T.) light-weight cryptography method was described in Ref. [24]. It is a 64-bit block cipher that requires data to be encrypted with a 64-bit address.

A New Lightweight Cryptographic Algorithm for Security Data was provided in the research [25] which might be utilized to secure cloud computing systems. The methods encrypt data with a 16-byte (128-bit) block cipher and a 16-byte (128-bit) key to enhance the encryption's complexity.

Many lightweight block ciphers are proposed for low resource devices and their design should resist against various attacks, as shown in Table 1 all these related works focus on implementing the lightweight block ciphers on different hardware platforms to determine their energy efficiency.

3. The proposed algorithm

This section discusses the proposed technique, a novel variation of cryptography algorithm that combines two levels of encryption to enhance cloud computing security. The first layer is a new effective light-weight cryptographic algorithm, namely (N.E.L.C.) and the second layer multiplicative homomorphic property of the R.S.A. algorithm. This approach offers both symmetric and asymmetric cryptography features, which improves cloud computing security and privacy. The following subsections describe this algorithm.

3.1. Description

Two levels of encryption are merged in the proposed technique. As illustrated in Fig. 3, the first layer is built on a symmetric-key algorithm and (substitution/permutation) structural approaches inspired by Feistal mixed with Shannon's theory (diffusion/confusion) by the participation of logical operations such as (XOR, XNOR, shifting, sapping).

The second layer is based on asymmetric cryptography. This kind of encryption allows specific forms of computations to be performed on encrypted text in order to get an encoded result that matches the product when decoded operations are done on the plain text. The RSA algorithm's multiplicative homomorphic feature is developed to increase data security in cloud computing.

In addition, the second layer method modifies RSA with homomorphic encryption algorithm implementation. The security of untrusted applications or systems is improved by using a homomorphic encryption technique. It converts the data into cipher-text, which is then decrypted [36]. It functions as though it were still in its original state. It enables the execution of sophisticated mathematical operations on encrypted data.

The formation and conceptual workflow of the proposed algorithm are presented in Fig (1). Two processes are provided for the conceptual demonstration, i.e. uploading and downloading of data from cloud storage; the first data input is encrypted and downloaded to the cloud through the encryption system. Downloading data from cloud storage reverses a similar method. There are three steps for the proposed encryption algorithm.

1. Key Generation Process
   - First Layer
   - Second Layer
2. Encryption Process
   - First Layer
   - Second Layer

3.2. Encryption layer 1: the new effective lightweight cryptographic algorithm

To improve cloud computing stability while maintaining high

Table 1
Summery of the Common Lightweight Cryptography algorithms.

Existing works	Contributions	Methodology	Short coming	R#
Deukjo 2006 HIGH	new block cipher HIGHT low-resource sensors a	HIGHT's structure is generic. Feistel and Network of Substitution-Permutation (SPN)	HIGHT is a 64-bit block cipher with a 128-bit key length	[26]
Zheng 2012 KLEIN	a new family of lightweight block ciphers wireless sensors/RFID	Substitution-Permutation Network (SPN)	It has a straightforward structure with an involutive S-box.	[22, 27]
Biswas et al. 2014	Simple lightweight encryption scheme Pseudorandom pattern	Elliptic curve over prime field	Computational time increases with the range of elliptic curve extended	[28]
Kalaiselvi & Mangalam 2015	Architecture based on AES algorithm	Key expansion approach Dual stage design	No security analysis	[29]
Biswas et al. 2015	Discrete chaotic map Genetic operations Text and image encryption	Elliptic curve over prime field Mutation and crossover	Smaller network Lesser throughput	[30]
Dridi et al. 2016	Chaotic neural network for image encryption	DICOM images Logistic Map (LM)	Limited range of key space	[30]
Gangadari & Ahamed 2016	AES algorithm low-power S-box architecture	Cellular automata of second order	No differential cryptanalysis	[31]
Baskar et al. 2016	Chaotic key generation algorithm	Modified XTEA Randomized key generation	No security analysis	[32]
Jian 2011 LED	LED is a novel 64-bit block cipher with two major instances that accept 64- and 128-bit keys.	Sboxes. LED cipher re-uses the present Sbox MIX round	Limited range of key space Mix Columns Serial	[33]
SIT	a new 64-bit block cipher 64-bit key cipher wireless sensors and RFID	Substitution-Permutation Festial	key cipher complex	[24]
NLCA	NLCA a symmetric key block cipher	To increase the encryption's complexity, a hybrid of SP and Feistel architectural techniques is used.	less memory	[34]
RC6	RC6, a descendant of RC5, was created. It was one of the five finalists and was designed to meet the standards of the AES contest.	Festial	Key length can be increased to 2048 bits.	[35]

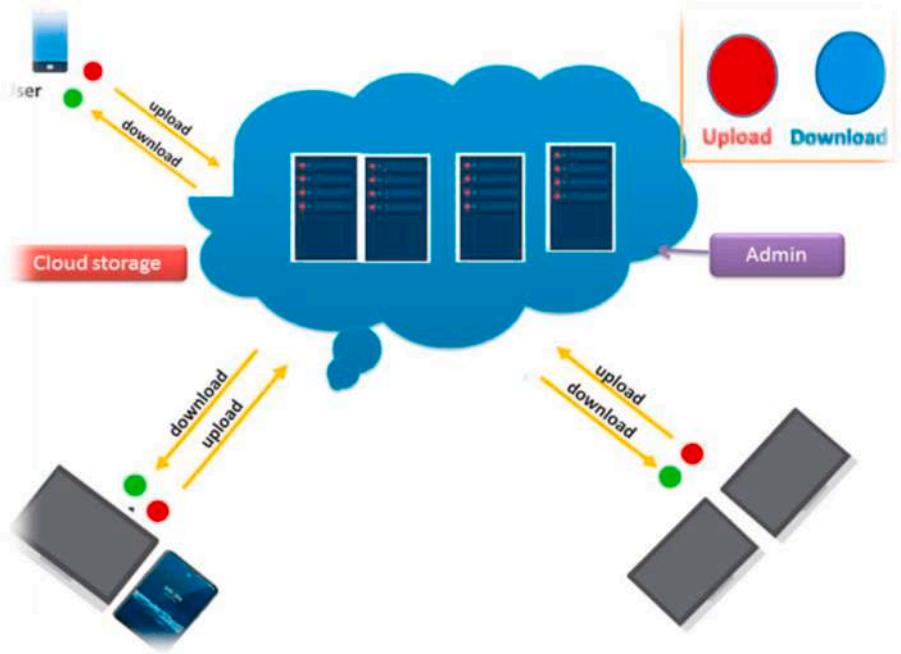

Fig. 1. The structure and conceptual workflow of the proposed model.

performance and low processing. The new proposed algorithm has implemented the basic Boolean operations such as XOR, Ex-NOR operations and sequencing. The algorithm combines the Feistel structure features with Network substitution-permutation (S.P.) features to increase the confusion and diffusion, improving the encryption complexity.

The core idea of this algorithm is to use an 8–16 byte (64/128-bit) block encryption and an 8-16-byte (64/128 bit) key to encrypt the data in a symmetric key technique, crypto rounds are required; each round depends on mathematical functions to produce diffusion and confusion. To ensure the encryption process strong enough to fulfill devices standards, encryption techniques are often designed to take 10 to 20 rounds on average. The proposed approach is restricted to 7 rounds to improve energy efficiency, with each cycle requiring crypto involving 32 bits of data to execute. The security is high due to the use of both the S.P and Feistel architectures. Furthermore, the mixed operations in this algorithm are provided in several algebraic functions, including XOR, XNOR, F.function and addition operations to create complexity for the attackers.

The procedure's detailed steps are outlined below.

1) Key Expansion Block.
2) Encryption Block.
3) Decryption Block.

3.2.1. Key Expansion Block

The key is the critical component of the algorithm in the process of encryption and decryption. The diffusion and confusion techniques used to generate the proposed algorithm strengthen the key. The strength of key generation results in increased

security, better encryption complexity, and decreased knowledge of the key by attackers. Two keys will be generated from the Key. The first will be used to decrypt the data, while the second will be used as an entry key in the key expansion process. The key expansion requires a 128-bit length, and the key is split into seven sub-keys (K1, K2, K3, K4, KK1, KK2, SK). The expansion key process is shown in pseudocode algorithm (1) and Fig. 2.

3.2.2. Encryption block process

The technique used for converting data from an identifiable type into an understandable form using diffusion and confusion strategies is named cryptography. Decryption is converting data from an unfamiliar format to a form that users can understand with authority to do so. The encryption block process is shown in pseudo code (2) and Fig. 4. The algorithm works on seven rounds to reduce energy usage. Each round is based on basic arithmetic to increase the security rate. Each round's output is the input for the next round to get the cipher text (C.T).

Pseudocode algorithm (1): Key Expansion

Input: 128 bit (k)
Output: 64 bit (kc)

1. **128-bit key divided to 64 R bit right,64 L bit left**
2. **in the 64 R divided into a group of 16 bit**
   - **p1 → 16 Bit shift process then feed 16 M matrix**
   - **p2 → 16-bit shift process then feed to F. Function**
   - **K1 = P1 ⊕ P2+ P2**
   - **p3 → 16 Bit shift process then feed to F. Function**
   - **p4 → 16 Bit Shift Process**
   - **K2 = P1+P4**
   - **KK=K1 ʘ K2**
3. **The 64 L divided into a group of 16 bit**
   - **p1 → 16 Bit shift process then feed to F. Function**
   - **p2 → 16 Bit Shift Process**
   - **K3 = P1+P4**
   - **p3 → 16 Bit shift process then feed 16 M matrix**
   - **p4 → 16-bit shift process then feed to F. Function**
   - **K4 = P1 ⊕ P2+ P2**
   - **KK1 =K3 ʘ 64**
4. **SK=KK+KK1**
5. **Output Key Expansion K1, K2, K3, K4, K.K., KK1, SK.**
6. **End**

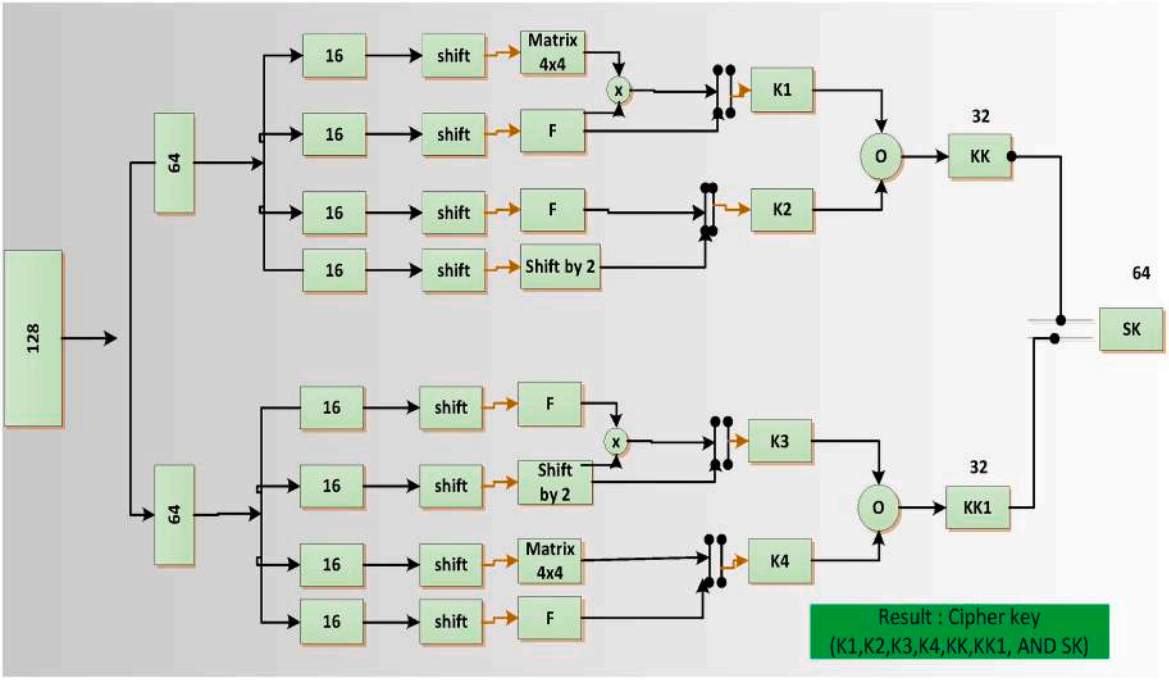

Fig. 2. Key expansion block process.

3.2.3. F-function

The F-Function approach consists of numerous non-linear and linear operations that ensure the complex dependence of output bits on input bits [22,37]. This mechanism, referred to as disorientation and diffusion, depends on the P and Q values seen in seen in Tables 2 and 3 and Fig. 3.

3.2.4. Decryption block process layer 1

The cryptographic algorithm decrypts the Ci cipher-text block, which is similar to the cryptography procedure in Mi block.

The Ci Block 128-bit is first divided into four sub-blocks, which are then altered using a combination of XOR and Sub operations with the same working keys. And, because they are the inverse of the encryption procedure, it is not essential to lay out the specific stages for the process. The decryption block procedure is depicted in Fig. 5.

The Pseudocode algorithm (2) explain the Encryption process steps.

***Pseudo code algorithm (2)**: Encryption process*

Input: 128 bit (plaintext and 128 key)

Output: 64 bit (cipher text)

1. ***Read the byte value from the input file***
2. ***Convert the input value to binary***
3. ***The block cipher is split into four sub-block32-bit sub-blocks each,*** *M1= 1-32, M2 33-64, M3= 65-96, and M4 = 96-128.*
4. ***Round1 Steps:*** *perform XOR operations between* ***(K1 ⊕M1),*** *then performs* ***M1 ⊕M2, M2 ⊕ M3****, M3 feed* ***F.Function*** *then* ***XNOR Output of F with M4 (F.F ʘ M4). As shown in figure 4 .Round 1 (R1).***
5. *The swapping process takes place* ***(M1, M2) and (M3, M4).***
6. ***Round 2 Steps:*** *performs XOR operations between* ***(K2 ⊕M4)*** *from* ***the left*** *then performs* ***XOR (M4 ⊕M3), M3*** *feed* ***F.Function*** *Then* ***output of F. (F.F ⊕ M2),*** *then XNOR* ***(M2 ʘ M1). As shown in figure 4 .Round 2 (R2).***
7. ***Round3 Steps:*** *perform XOR operations between* ***(K3 ⊕M1),*** *then performs (M1 ⊕M2, M2 ⊕ M3), M3 feed* ***F.Function*** *then* ***XNOR the*** *Output of* ***F with M4 (F.F ʘ M4). As shown in figure 4 .Round 3 (R3).***
8. *The swapping process takes place* ***(M1, M2) and (M3, M4).***
9. ***Round 4 Steps****: perform XOR operations between* ***(K4 ⊕M4)*** *from* ***left*** *then performs* ***XOR (M4 ⊕M3), M3*** *feed* ***F.Function*** *Then* ***output of F. (F.F ⊕ M2),*** *then XNOR* ***(M2 ʘ M1). As shown in figure 4 .Round 4 (R4).***
10. ***Round5 Steps:*** *perform* ***XOR*** *operations between K.K. and M1* ***(K.K ⊕M1),*** *then performs (****M1 ⊕M2, M2 ⊕ M3****), M3 feed F.Function Then* ***output of F. (F.F ʘ M4). As shown in figure 4 .Round 5 (R5).***
11. *The swapping process takes place* ***(M1, M2) and (M3, M4).***
12. ***Round 6 Steps:*** *performs* ***XOR*** *operations between KK1 and M4* ***(KK1 ⊕M4)*** *from left and then performs XOR* ***(M4 ⊕M3),*** *M3 feed F.Function Then* ***output of F (F.F ⊕M2),*** *then* ***(M2 ʘ M1). As shown in figure 4 .Round 6 (R6).***
13. ***Combine M1, M2 and M3, M4 MP1= M1 + M2 MP2 = M3 +M2.***
14. ***Round 7 Steps:*** *perform XNOR operations between SK. and MP1* ***(SK ⊕MP1),*** *then XNOR operation performs (****MP1 ʘ MP2)*** *then C= MP1+ MP2.*
15. ***Layer 1: cipher text produces.***
16. ***Convert binary to decimal***
17. *Applied LAYER 2;* ***Multiplicative Homomorphic property of R.S.A. Algorithm***
18. *Upload to cloud.*
19. *E.N.D.*

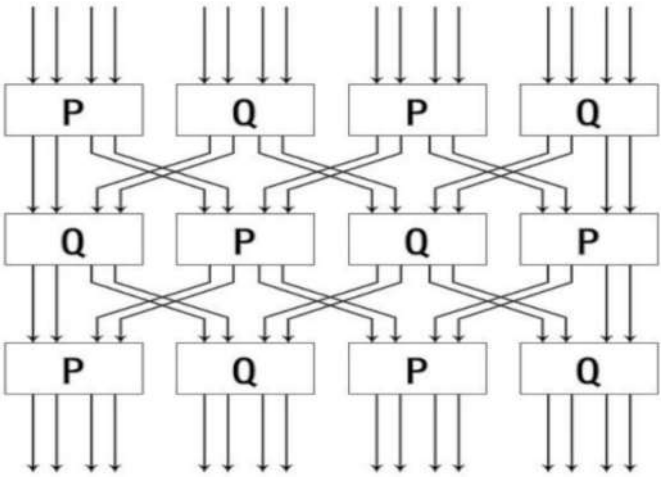

Fig. 3. F-function [30].

3.3.3. Encryption layer 2: multiplicative homomorphic property of RSA algorithm

Homomorphic encryption is one good idea that performs arbitrary computations on data without ever decrypting it. In 1978, performing computations on encrypted data was proposed by Ron Rivest, Adleman and Dertouzos to promote the idea of hiding the data. The capacity of performing computations gave rise to several useful applications. This also included outsourcing arbitrary values privately in the cloud to store the resultant encrypted text, carry computations on ciphered data and decrypt only when necessary.

Homomorphic encryptions are of two types: fully homomorphic and partially or "somewhat homomorphic scheme". A completely homomorphic encryption scheme allows for potentially sophisticated operations on ciphered data. It performs both addition and multiplication operations on encrypted data. Somewhat or partially homomorphic encryption scheme allows either multiplication or addition operation on encrypted data, but not both.

In the field of cloud security, the application of homomorphic encryption is an important milestone. It is possible to outsource sensitive data with computations on the cloud server by keeping the secret key for decryption [38]. A multiplicative homomorphic system's encryption function has the following characteristics: M1 and M2 are plaintext messages, hence E(M1) *E(M2) = E(M1*M2). Data processing, cloud computing, electronic voting, and financial transactions are just a couple of minor applications for homomorphic encryption [7]. The RSA algorithm is depicted as an illustration for multiplying homomorphic algorithms in the following description [39].

Encryption/Decryption process of Multiplicative RSA Algorithm.

- *Generation of the Key*
- *Choose two large primes, p and q, such that*
  (p q. n = p * q. φ (n) = (p-1) *(q-1), where φ is Euler's totient function.
- *Select an integer e such that* $1 < e < \varphi(n)$ *and gcd* $(e, \varphi(n)) = 1$ *(co prime).*
- $d = e^{-1} \bmod \varphi(n)$
- *Public key ((e,n))*
- *Private key d*
- *Encryption* $c = m^e \bmod n$
- *Decryption* $M = C^d \bmod n$

The RSA algorithm's multiplicative homomorphic characteristic is as follows [19]:

Given in (1)

$C1 = M_1{}^E$ M.O.D. N,

$C2 = M_2{}^E$ MOD N

$C1.C2 = E_{PK}(M_2).E_{PK}(M_2) = M_1{}^E M_2{}^E (\text{MOD N}) = (M_1.M_2)^E (\text{MOD N}) = E_{PK}(M1.M2)$.

4. Simulation and implementation environment

Omnet C++ v6 was developed to implement a proposed algorithm made in a private cloud Omnet installed on the DELL Inspiron 13 7000 series on an Intel CoreTM i7-3120 M processor, 2.50 GHz 16G.B. RAM. Three groups are utilized to generate clouds with enough node numbers (owners/users) to display each node.

In iCanCloud few classes have been modified, namely Power host, VMScheduler, VM, and Cloudlet Scheduler for simulation purposes to realize dynamic resource allocation and class dynamic memory. Dynamic memory was newly added to guess the required resource. This class also updates virtual machine resources after cloudlet implementation.

Algorithms have been implemented in MAT.LAB. and applied in C++ using the Dev. C++ program, as illustrated in Figs. 6 and 7. The Different parameters have been evaluated, i.e. (execution time, throughput, key size encryption/decryption, length Cipher-text, and security standard. In the following part, a performance efficiency analysis is also carried out for comparison.

5. Results and discussion

Several security experiments are performed to verify the algorithm's quality, compared to other lightweight encryption algorithms and current symmetric and asymmetrically key encryption techniques such as A.E.S., D.E.S. and Blowfish R.S.A., E.G.A.M.A.L. The analysis of the two algorithms is below. We experimented with different file sizes in kilobytes (K.B.) as well as time estimates for encryption and decryption (milliseconds).

5.1. Evaluation parameters

Very well-known parameters used to analyses the security of the encryption for the proposed algorithm are:

- Avalanche test

A significantly relevant parameter for analyzing the encryption algorithm's security (randomness). The avalanche experiment is used to verify the cryptography scheme's sensitivity and to alter the initial conditions. This indicates that a minor change in the encryption key should result in a different cipher text. In this case, the assessment is considered optimal if 50% of the bits are changed due to a single bit of modification according to the Strict Avalanche Criteria (S.A.C.) [40]. We decrypt the image using a key that differs by one bit from the correct one to detect this effect visually. As seen in Fig. 6 above, the proposed algorithm can cause a significant number of bits to move. This may be attributed to transferring a single bit of picture/text or key bits like a landslide. The proposed algorithm 128-bit avalanche is 51.55%.

- Time complex

With a 128-bit key size, the attacker would need to find 2^{128} possible keys. As a result, the time complexity of 2^{128} for obtaining the proper key is O on average (1). In reality, the proposed algorithm has a time complexity comparable to AES, but it is more efficient since there are no more repetitions than A.E.S. and the rest of the similar algorithms.

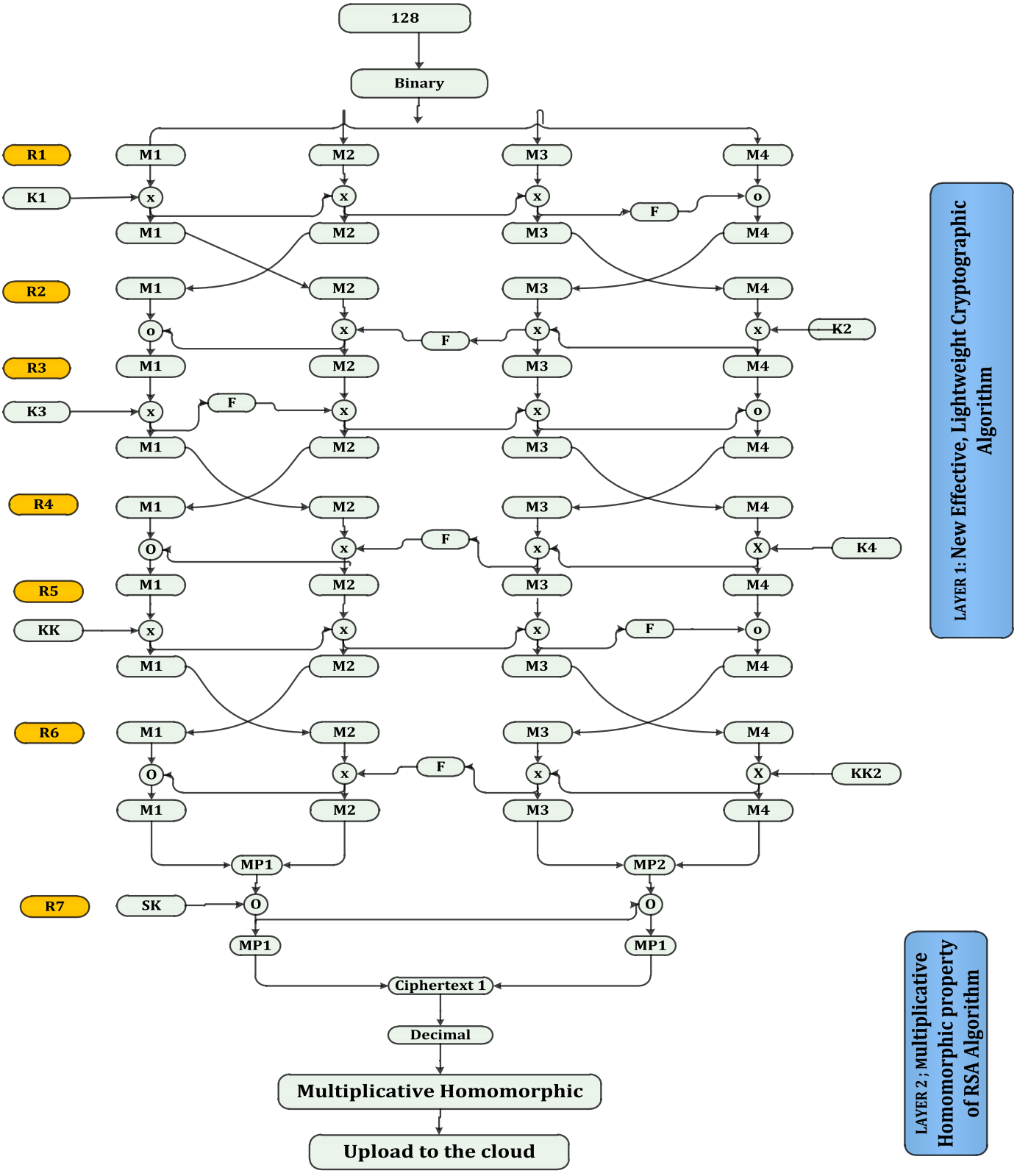

Fig. 4. Encryption process steps.

Table 2
(P) Table.

Kc	0	1	2	3	4	5	6	7	8	9	A	B	C	E	D	F
P(KC)	3	F	E	0	5	4	B	C	D	A	9	6	7	8	2	1

Table 3
(P) Table.

Kc	0	1	2	3	4	5	6	7	8	9	A	B	C	E	D	F
Q(KC)	9	E	5	6	A	2	3	C	F	0	4	D	7	B	1	8

- Execution time

One of the most crucial aspects to consider while building cryptography is execution time. The overall time taken to encrypt/decrypt the unique data is known as the encryption cryptographic execution time. This cryptography algorithm was implemented in dev C++ and MAT. LAB. R2016a. The evaluation test has done in the text in different size and on the grayscale image "Peppers", "panda" of size 128*128, 256 × 256 The experiment was performed 10 times as plain images Table 4 shows the average time to execute the encryption and decryption process for text and Table 5 for the image. The tables indicate the execution time in milliseconds of equivalent algorithms with various file sizes. It is obvious that the proposed algorithm takes less time than the other algorithms.

- Throughput

The throughput rate can be used to evaluate the algorithm's effectiveness. The algorithm's throughput is directly related to its performance; the higher the performance/the higher the throughput. The formula for calculating the transfer rate of encoder technology is as follows.

Throughput = Plain Text Size/Encoding Time.

5.2. Statistical analysis

- Image Entropy

Information entropy analysis: the encryption algorithm applies extra information to the details, such as the discrepancy between the original data and the algorithm used, which is complicated for the attacker. The entropy of an image It's a straightforward parameter to evaluate the randomness of the encrypted image. This parameter computes the difference in entropy between the original and encrypted image. The higher the entropy modification, the better the encryption. The following equation can be used to compute the entropy.

$$\boldsymbol{E} = \sum_{1}^{N} \boldsymbol{i} = 1\ \boldsymbol{Xi}(\boldsymbol{log}2(\boldsymbol{Xi})) \quad (1)$$

Where "E" stands for image entropy, "X" stands for the probability of each degree of intensity in the image, and "N" stands for the total number of degrees of intensity in the image.

- Image Histogram

In recent times, histogram analysis has utilized a parameter that depicts the randomness of the distribution of encrypted picture data. In order to comprehend the average change in the strength of the encrypted information, the histogram of encrypted and unencrypted photos corresponds with this measure. The main object of the histogram analysis is to show the properties of ciphered data uncertainty and diffusion. Fig. 8. Display the study of the histograms.

- Correlation analysis

Correlation is an effective method to evaluate out how strong a cryptographic algorithm is. In this study, the connection between the encrypted data and the original data is cs evaluated. A effective encryption approach will ideally result in encrypted data with 0% overlap. The analysis of correlations seen in Table 5 and Fig. 9.

6. Comparative analysis

In this section, comparative studies are conducted to present and verify the proposed algorithm's feasibility and describe the analysis of the difference between the proposed algorithm, namely (N.E.L.H.C.) with a homomorphic, light-weight, symmetric and asymmetric encryption algorithm that is commonly used for cloud computing security. The comparative studies divided into two sections describe the following.

6.1. Comparative analysis of the proposed algorithm with a light-weight cryptographic algorithm

The first section was conducted, taking into account some evaluated parameters commonly

used for evaluated the encoding and decoding processes, such as Block Size, execution time, Key Length, Possible Key, Mathematical Operations, Cipher Type and Security Power parameters, as shown in Table .6 and Fig. 10.

6.2. Comparative study of some symmetric and asymmetric algorithm

The proposed algorithm was compared to several symmetric and asymmetric encryption algorithms frequently used for security information in cloud computing in the second section.The comparative study

based on evaluated parameters commonly used for evaluated the Enc/Dec processes, such as Structure, Key size, Block Size, Possible Key, Execution Time, Cipher Type and Security Power parameters, as shown in Table 7.

7. Security analysis and C.I.A. Achievements

The strength of any cryptographic process depends on its sustainability. The attacker usually attempts to begin different possible forms of attack in order to compromise the information's confidentiality. In particular, it attempts to with brute force attack, Weak Key Attacks, and Square Attack for cipher parsing.

7.1. Brute force attack

A brute force attack is when a hacker attempts to find keys by utilizing an alternative space. As the space utilized by the switches is in a 16-bit block multi-block structure, n is the space of $n*2^{128}$-bit with n being the number of blocks. The keys cannot be mathematically measured. Moreover, even if one of these keys is trusted, the weight of 2^{128} needed to build the remaining keys cannot be estimated. Therefore,

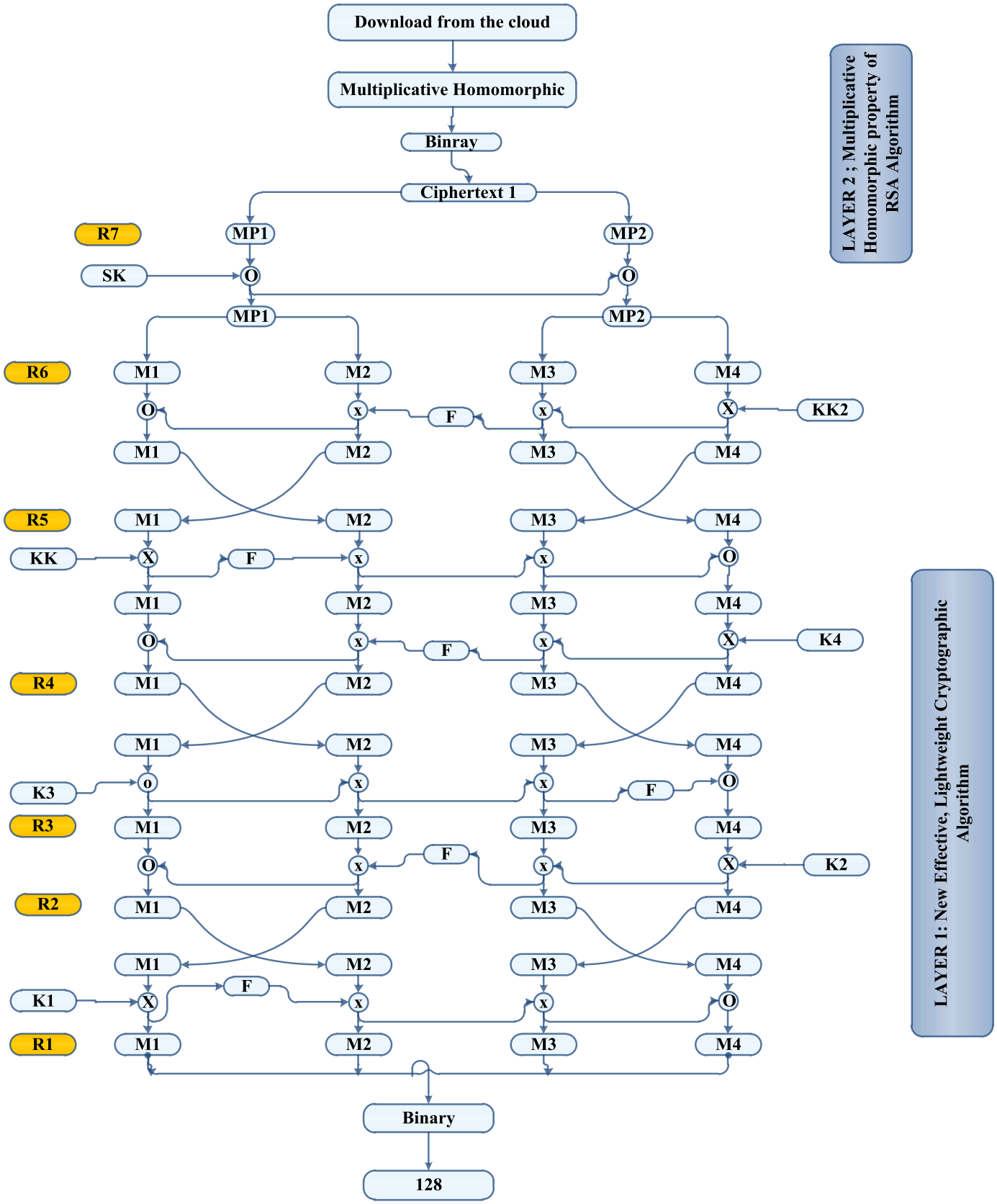

Fig. 5. Decryption process step.

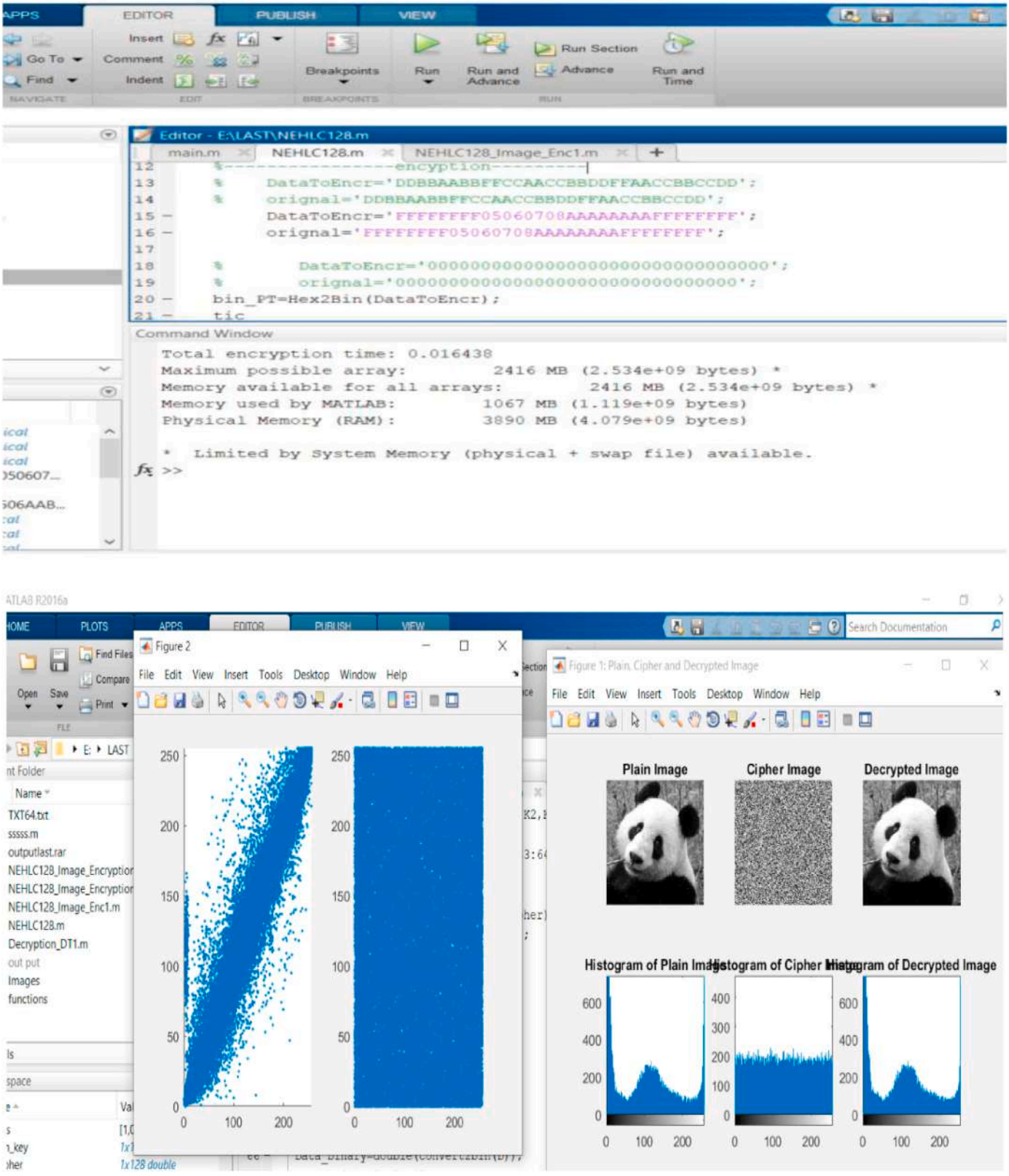

Fig. 6. A, B. Implemented process in M.A.T.L.A.B.

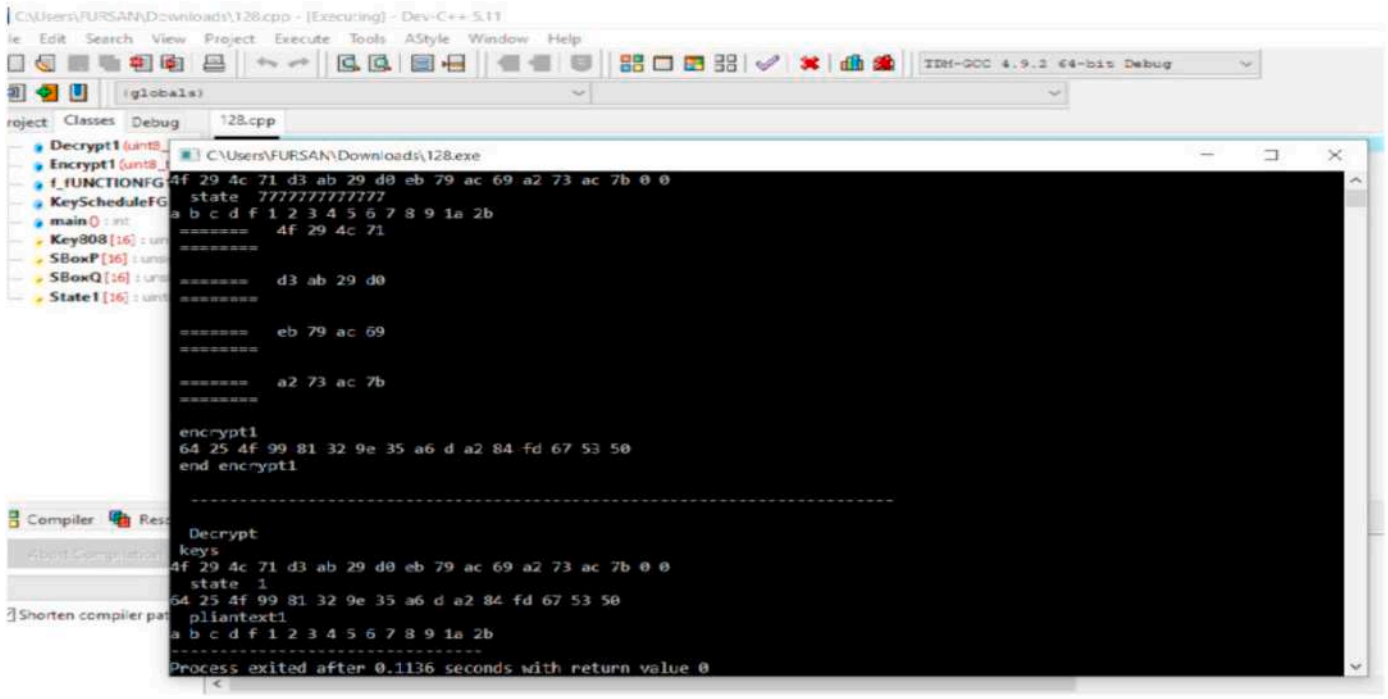

Fig. 7. Implemented process in Dev. C++.

Table 4
Processing time algorithm.

Plaintext Size (KB)	Enc/Dec Time (S)	Throughput (Kb/Sec)
255 kb	0.67	380.94
500 kb	0.93	537.63
750 KB	1.13	842
1 MB	2.88	663.71
Average	1.4	606

Table 5
Shows the Statistical Analysis (Image encryption, Image histogram, Correlation).

No	Image	Image Size	Correlation		UACI	NPCR
			original	encryption		
3	Banda	128	0.9000	0.0021	22.6	99.6052
		256	0.9807	0.0031	31	99.6345
4	Peppers	128	0.9601	0.0011	24.8	99.5231
		256	0.9309	0.0031	33	99.6231

the proposed cryptographic scheme prevents a brute assault by force.

7.2. Linear and differential cryptanalysis

Linear and differential attacks are absolutely unsuccessful when completely encrypted. That is, the new f-function works the same thing in Ref. [30]. If you use the linear approximation for two rounds, the ratio of input and output is very strong. Circular transformation is often maintained uniformly, comparably treating any bit and opposing differential attacks.

7.3. Weak Key Attacks

Encryption is considered strong if the algorithm generates strong encryption keys. The actual key provides the encryption key. The real key to XORing protects against this attack before it is used. The same applies to S.I.T [30]. and cipher [8], which has shown security against weak keys. In this way, the algorithm uses F-Function and then uses operations (XNOR, XOR) to maximize complexity (confusion and diffusion). The algorithm, thus, thwarts this sort of attack.

7.4. C.I.A. Achievement

- Confidentiality

This indicates that unauthorized individuals are involved when information is shared. The suggested solution establishes confidentiality by encrypting all transmitted entities and parameters.

- Data integrity

ensures that no modifications are made to the user as a result of insertion, deletion, or alteration. In other words, although the data has been manipulated, the receiver should offer specific processes to ensure that new information is obtained. Data integrity was achieved in this approach via segmentation.

- Availability

This means to ensure availability and access knowledge to users wherever the need arises. The suggested cryptographic algorithms are hypothetical techniques and are therefore useable at all times. It also supports text formats for broadband data encryption and decryption without loss of information, without losing any scheme where not lost any bit during transmission. The scheme also tests the proposed algorithm encryption using the white spaces and special characters sizes up to 10,000 plain text character.

8. The conclusions and further recommendations

Cloud computing has grown in popularity among businesses due to its remote connectivity, lower costs, and fast re-provisioning. Although users are enthusiastic about this new computing model, they are also worried about the security threats associated with the cloud. There are

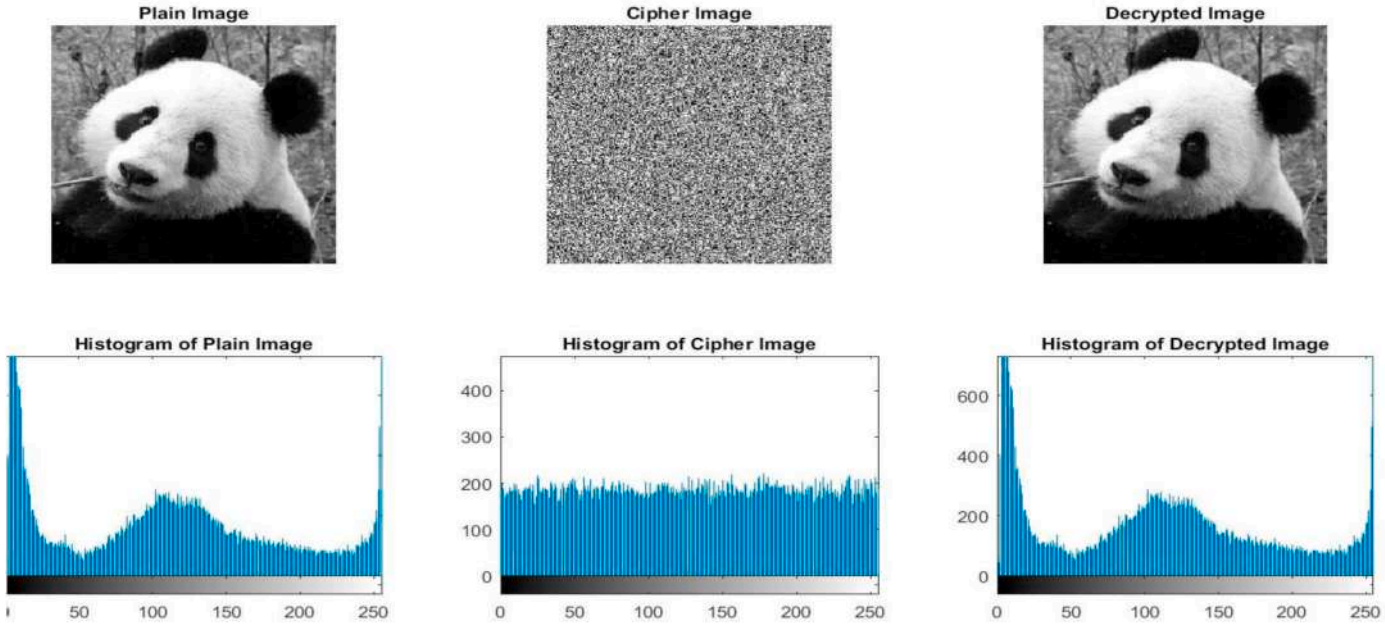

Fig. 8. Show the Image encryption and Image histogram.

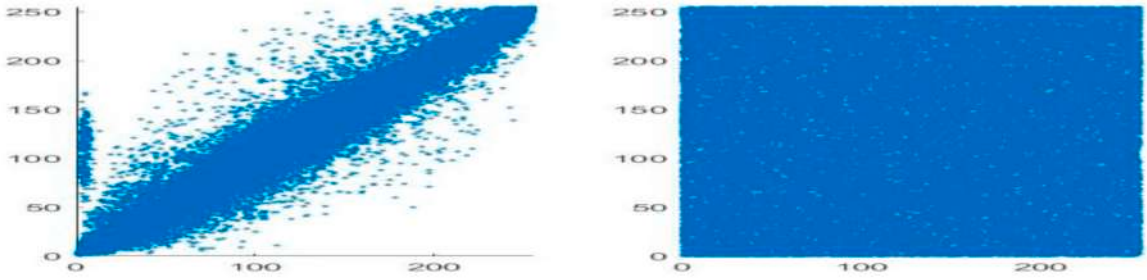

Fig. 9. Show the Correlation analysis.

Table 6
Comparison in terms of Flexibility, Architecture, Security and Limitation.

Algorithm	HIGHT [26]	SEA [41]	LED [42]	RC6 [35]	NLCA [25]	PROPOSED ALGORITHM
	symmetric	symmetric	symmetric	asymmetric	symmetric	symmetric/asymmetric
Structure	Feistel	Festial	Festial	Festial	Festial + SP	Festial + SP + Multiplicative Homomorphic
Layer	1	1	1	1	1	2
Block size	64 bits	48, 96, 144 bit	64 or 128	128 bits	128, or 256	32,64,128
Key size	128 bits	48, 96, 144 bit	64 or 128	128, 192, 256 bits	128,256	64,128
No. of Round	32	Variable	Variable	20	4	4
Possible key	2^{56} bits	2^{48}, 2^{96} Or 2^{144} bits	2^{64},2^{128} bits	2^{128},2^{196} bits	2^{128},2^{256} bits	2^{32},2^{64},2^{128},
Average Enc/Dec time (S)	2.4	4.2	2.9	2.63	1.89	1.66
Mathematical	Addition, subtraction, XOR, Shifting. (8 bits)	XOR, rotations, 2n mod addition, substitution (8 bits)	XOR, rotations, 2n mod addition, substitution (6 bits)	Addition (2's comp). Variable Rotation, XOR, (16 bits)	Shifting, Substitution (4 bits) XOR, XNOR,	Shifting, Substitution (16 bits) XOR, XNOR,
Security rate	Secure	Secure	Secure	Secure	Secure	Highly Secure

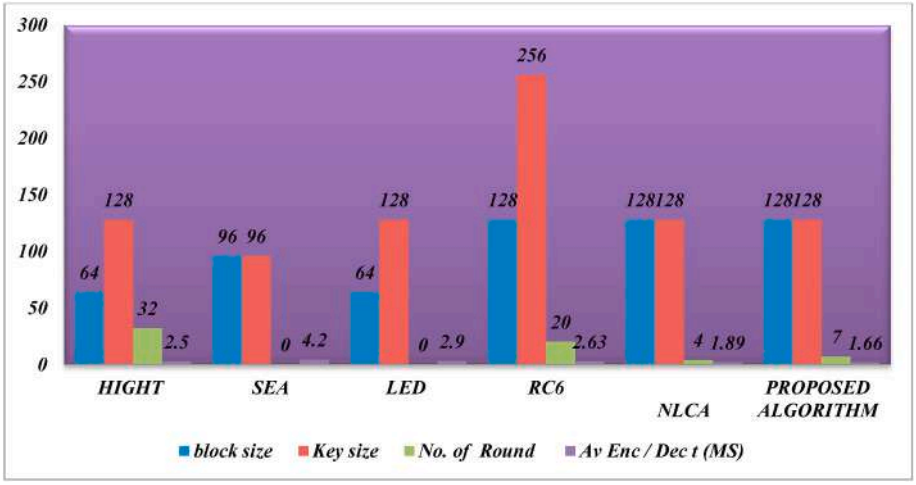

Fig. 10. Demonstrate the suggested technique's comparative analysis with a light-weight cryptographic technique.

Table 7
Comparative study of some of the symmetric and asymmetric algorithm.

	AES [43]	BLOWFISH [44]	*SIT* [24]	HOMOMORPHIC RSA [7]	HOMOMORPHIC ELGAMAL [7]	PROPOSED ALGORITHM
Structure	Subs-Per	Festial	Festial/SP	modular exponentiation	modular exponentiation	Festial/SP/modular exponentiation
Algorithm	symmetric	symmetric	symmetric	asymmetric	asymmetric	symmetric/asymmetric
Key Size	128 bit	64 bits	64	Key Bit Random	Key Bit Random	128/256/512/1024
Block Size	128, 192, 256 bits	32–448 bits	64	512/1024	512/1024	128/256/512/1024
Key space analysis	2^{128}, 2^{192} Or 2^{256} bits	2^{32}–2^{448} bits	264	Random	Random	2^{128},$2^{256,512,1024}$ bits
Deposit Of Keys	needed	needed	needed	no	no	needed
No. Of Round	10, 12, 14	16	5	Random	Random	layer 1 = 4 layer 2 = 3
Encryption Process	Moderate	Moderate	Faster	faster	Moderate	Faster
Decryption Process	Moderate	Moderate	Moderate	faster	Moderate	Faster
Power Consumption	Low	Low	Moderate	high	high	High
Security	Secure	Secure	Secure	Secure	Secure	High Secure

still many obstacles to data protection and privacy that must be overcome. Since the cloud provides flexible and easy-to-manage access to data storage, there is still the possibility of unauthorized attacks and malicious activities. As a consequence, new encryption techniques and methods for enhancing cloud storage security must be improved.

In the suggested research, a Novel Effective Lightweight Homomorphic Cryptographic Algorithm contains two layers of encryption to enhance data secrecy.

The first layer A novel 128-bit Lightweight cryptography technique depends on feistal and permutation/substitution architectural process with Shannon's theory of diffusion/confusion based on the involving of logical operations, such as (XNOR, XOR, swapping, shifting) to improve the complexity of the encryption which use in the first layer of encryption and the second layer is the multiplicative homomorphic property of the R.S.A. algorithm for enhancing data security.

The result of the proposed algorithm outperforms another Lightweight Cryptographic Algorithm. (HIGHT, SEA, LED., RC6, and NLCA) and some of the symmetric and asymmetric algorithm (AES, BLOWFISH, SIT, HOMOMORPHIC RSA, HOMOMORPHIC ElGamal) in regard to the size of the ciphertext, encryption time, throughput, and security level.

The proposed encryption algorithm has experimentally validated for brute force, encrypted text only, known-plaintext attacks and differential cryptanalysis attacks. It's been put to the test on a variety of data, including whitespace and special characters. The C.I.A. principle is also met by the proposed encryption technique. The suggested technique might be implemented in hardware (cloud-based IoT) in the future, resulting in significantly better outcomes.

Declaration of interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Acknowledgements

This research was supported by the Ministry of Higher Education – Yemen. The authors would like to thank Prof. Dr Sudhir B. Jagtap S.R.T. M University India for his guidance.

References

[1] M.A. Hossain, A. Ullah, N.I. Khan, M.F. Alam, Design and development of a novel symmetric algorithm for enhancing data security in cloud computing, J. Inf. Secur. (2019), https://doi.org/10.4236/jis.2019.104012.
[2] G. Viswanath, P.V. Krishna, Hybrid encryption framework for securing big data storage in multi-cloud environment, Evol. Intell. (2020), https://doi.org/10.1007/s12065-020-00404-w.
[3] B.A. Sullivan, Securing the cloud: cloud computer security techniques and tactics, Secur. J. (2014), https://doi.org/10.1057/sj.2012.16.
[4] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Generat. Comput. Syst. (2012), https://doi.org/10.1016/j.future.2010.12.006.
[5] Z. Kartit, et al., Applying encryption algorithm for data security in cloud storage, Lecture Notes in Electrical Engineering 366 (2016) 141–154, https://doi.org/10.1007/978-981-287-990-5_12.
[6] M. Tebaa and S. El Hajji, "Secure cloud computing through homomorphic encryption," vol. 5, no. December, pp. 29–38, 2014, [Online]. Available: http://arxiv.org/abs/1409.0829..

[7] I. Jabbar, Using fully homomorphic encryption to secure cloud computing, Internet Things Cloud Comput. 4 (2) (2016) 13, https://doi.org/10.11648/j.iotcc.20160402.12.
[8] W. Zhang, Z. Bao, D. Lin, V. Rijmen, B. Yang, I. Verbauwhede, RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms, Sci. China Inf. Sci. (2015), https://doi.org/10.1007/s11432-015-5459-7.
[9] R. Amin, N. Kumar, G.P. Biswas, R. Iqbal, V. Chang, A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment, Future Generat. Comput. Syst. 78 (2018), https://doi.org/10.1016/j.future.2016.12.028.
[10] R. Arora, A. Parashar, Secure user data in cloud computing using encryption algorithms, Int. J. Eng. Res. Afr. 3 (11) (2013).
[11] A. Dhamija, V. Dhaka, A Novel Cryptographic and Steganographic Approach for Secure Cloud Data Migration, 2016, https://doi.org/10.1109/ICGCIoT.2015.7380486.
[12] A. Bhardwaj, G.V.B. Subrahmanyam, V. Avasthi, H. Sastry, Security Algorithms for Cloud Computing (2016), https://doi.org/10.1016/j.procs.2016.05.215.
[13] P. Chinnasamy, S. Padmavathi, R. Swathy, S. Rakesh, Efficient data security using hybrid cryptography on cloud computing, Lect. Notes Networks Syst. 145 (November) (2021) 537–547, https://doi.org/10.1007/978-981-15-7345-3_46.
[14] D.P. Timothy, A.K. Santra, A Hybrid Cryptography Algorithm for Cloud Computing Security, 2017, https://doi.org/10.1109/ICMDCS.2017.8211728.
[15] S. Belguith, L. Lip, Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm, no. c, 2015, pp. 98–103.
[16] K. Jakimoski, Security techniques for data protection in cloud computing, Int. J. Grid Distrib. Comput. (2016), https://doi.org/10.14257/ijgdc.2016.9.1.05.
[17] D.S. Abd Elminaam, H.M.A. Kader, M.M. Hadhoud, Evaluating the performance of symmetric encryption algorithms, Int. J. Netw. Secur. 12 (2) (2010), https://doi.org/10.1109/CSCI.2016.257.
[18] M. Louk, H. Lim, Homomorphic Encryption in Mobile Multi Cloud Computing, 2015, https://doi.org/10.1109/ICOIN.2015.7057954.
[19] J. Li, D. Song, S. Chen, X. Lu, A Simple Fully Homomorphic Encryption Scheme Available in Cloud Computing, 2013, https://doi.org/10.1109/CCIS.2012.6664399.
[20] M. Togan, C. Pleşca, Comparison-based Computations over Fully Homomorphic Encrypted Data, 2014, https://doi.org/10.1109/ICComm.2014.6866760.
[21] C. Moore, M. O'Neill, E. O'Sullivan, Y. Doroz, B. Sunar, Practical homomorphic encryption, A survey (2014), https://doi.org/10.1109/ISCAS.2014.6865753.
[22] Z. Gong, S. Nikova, Y.W. Law, KLEIN: A new family of lightweight block ciphers (2012), https://doi.org/10.1007/978-3-642-25286-0_1.
[23] T.P. Berger, J. Francq, M. Minier, G. Thomas, Extended generalized Feistel networks using matrix representation to propose a new lightweight block cipher: lilliput, IEEE Trans. Comput. (2016), https://doi.org/10.1109/TC.2015.2468218.
[24] M. Usman, I. Ahmed, M. Imran, S. Khan, U. Ali, SIT: a lightweight encryption algorithm for secure Internet of things, Int. J. Adv. Comput. Sci. Appl. (2017), https://doi.org/10.14569/ijacsa.2017.080151.
[25] F. Thabit, A. Prof, S. Alhomdy, A.H.A. Al-ahdal, Exploration of Security Challenges in Cloud Computing : Issues , Threats , and Attacks with Their Alleviating Techniques Exploration of Security Challenges in Cloud Computing : Issues , Threats , and Attacks with Their Alleviating Techniques, vol. 1, 2020. December.
[26] D. Hong, et al., HIGHT: A New Block Cipher Suitable for Low-Resource Device, 2006, https://doi.org/10.1007/11894063_4.
[27] W. Li, An ultra-lightweight side-channel resistant crypto for pervasive devices, Int. J. Multimed. Ubiquitous Eng. (2015), https://doi.org/10.14257/ijmue.2015.10.11.17.
[28] K. Biswas, V. Muthukkumarasamy, K. Singh, An encryption scheme using chaotic map and genetic operations for wireless sensor networks, IEEE Sensor. J. (2015), https://doi.org/10.1109/JSEN.2014.2380816.
[29] K. Kalaiselvi, H. Mangalam, Power efficient and high performance VLSI architecture for AES algorithm, J. Electr. Syst. Inf. Technol. (2015), https://doi.org/10.1016/j.jesit.2015.04.002.
[30] K. Biswas, V. Muthukkumarasamy, E. Sithirasenan, K. Singh, A Simple Lightweight Encryption Scheme for Wireless Sensor Networks, 2014, https://doi.org/10.1007/978-3-642-45249-9_33.
[31] B.R. Gangadari, S.R. Ahamed, Low power S-box Architecture for AES algorithm using programmable second order reversible cellular automata: an application to WBAN, J. Med. Syst. (2016), https://doi.org/10.1007/s10916-016-0622-2.
[32] C. Baskar, C. Balasubramaniyan, D. Manivannan, Establishment of Light Weight Cryptography for Resource Constraint Environment Using FPGA, 2016, https://doi.org/10.1016/j.procs.2016.02.027.
[33] J. Guo, T. Peyrin, A. Poschmann, M. Robshaw, The LED block cipher (2011), https://doi.org/10.1007/978-3-642-23951-9_22.
[34] S.B.J. Fursan Thabit, Alhomdy, A new lightweight cryptographic algorithm for enhancing data security in cloud, Glob. Transitions Proc. 2 (1) (2021), https://doi.org/10.1016/j.gltp.2021.01.013.
[35] R. Rivest, M.J.B. Robshaw, R. Sidney, Y.L. Yin, "The RC6 block cipher," first adv, Encryption ... (1998).
[36] D. Chandravathi, D.P.V. Lakshmi, Performance analysis of modified rsa and rsa homomorphic encryption scheme for cloud data security, Int. J. Adv. Res. 5 (2) (2017) 275–281, https://doi.org/10.21474/ijar01/3144.
[37] F. Muller, A new attack against Khazad, Lect. Notes Comput. Sci. (2003), https://doi.org/10.1007/978-3-540-40061-5_22.
[38] M. Rouse, RSA Algorithm (Rivest-Shamir-Adleman), TechTarget, 2014.
[39] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM (1978), https://doi.org/10.1145/359340.359342.
[40] A.F. Webster, S.E. Tavares, On the Design of S-Boxes (1986), https://doi.org/10.1007/3-540-39799-X_41.
[41] S.S.S.I. Huang, SEA: secure encrypted data aggregation in mobile WSNs, in: Int. Conf. Comput. Intell. Secur, IEEE, 2007, pp. 526–530, 2007.
[42] G. Bansod, N. Raval, N. Pisharoty, Implementation of a new lightweight encryption design for embedded security, IEEE Trans. Inf. Forensics Secur. (2015), https://doi.org/10.1109/TIFS.2014.2365734.
[43] M.A. Wright, The advanced encryption standard, Netw. Secur. (2001), https://doi.org/10.1016/S1353-4858(01)01018-2.
[44] M.N. Valmik, P.V.K. Kshirsagar, Blowfish algorithm, IOSR J. Comput. Eng. (2014), https://doi.org/10.9790/0661-162108083.

INTERNATIONAL RESEARCH JOURNAL OF HUMANITIES AND INTERDISCIPLINARY STUDIES
(Peer-reviewed, Refereed, Indexed & Open Access Journal)
DOI : 03.2021-11278686 ISSN : 2582-8568 IMPACT FACTOR : 6.865 (SJIF 2023)

Effectiveness of ICT in Teaching and Learning in Secondary School with respect to School Teachers in Pune District Area, using Evolutionary Algorithm Based Technique

Mr. Upendra Durgadasrao Choudhari
Ph.D. Scholar,
Swami Ramanand Teerth Marathwada University, Nanded (Maharashtra, India)
E-mail: udchoudhari2012@gmail.com

Dr. Sudhir Baburao Jagtap
Principal & Professor,
Vivekanand Mahavidyalaya, Udgir, Dist. Latur (Maharashtra, India)
E-mail: sudhir.jagtap7@gmail.com

DOI No. 03.2021-11278686 **DOI Link ::** https://doi-ds.org/doilink/03.2023-74982497/IRJHISIC2302053

Abstract:

The study investigated effectiveness of Information and Communication Technology (ICT) in teaching and learning in Secondary schools in Pune district area of Maharashtra State. A sample size of 236School Teachers was used for the study. Simple random sampling technique was used to compose the sample. To measure the effectiveness, researcher used three research questions were answered. Questionnaire method used for data collection, it was objectively used to investigate the utilization of ICT tools, how ICT tools are used to evaluate teaching learning process and the constraint to effective utilization of ICT tools by Teachers. The study attempts to fit a classification, recursive partitioning and regression trees i.e. CART method also chi-square test is used. "The decision tree method is a powerful and popular predictive machine learning technique that is used for both classification and regression" [1]. This method known as Classification and Regression Tree (CART) [2]. Also, researcher use a Chi-Square statically analysis was done to find the difference between area wise data from the schools. The R Software implementation is carried out for this study, this implementation of the CART algorithm is called RPART (Recursive Partitioning And Regression Trees). "Here researcher use R software coding to compute and process classification and regression trees." [3]It was found that ICT tools were not fully utilized in the school. Based on the findings, it was recommended among others that the government of Maharashtra should embark on a massive computer literacy training programme state wide particularly for the teachers at all level of education.

Keywords: *Information Communication Technology (ICT), Effectiveness, Information Technology (IT), Computer, Internet and Multimedia.*

1. Introduction:

Information Communication Technology (ICT) is to align with the global best practices, with this ICT occupied a central stage in the senior secondary school curriculum in order to presents the total experiences to which all teachers must exposed and through which the content and performance

objectives of the subject must be achieved for teachers. Also, the teaching and learning materials of any subject when provide, it enhances the effective teaching and learning. Thus, these could be possibly released if all the teachers can effectively integrate ICT into the classroom. As stated by Olelewe and Amaka (2011), a good teacher can use various teaching and learning technologies like computer, internet and multimedia resources, which are increasingly being used in support of the teaching and learning process in presenting new challenges and opportunities for teachers and students to translate information into relevant knowledge that a student can understand, keep it and pass on to others under a favorable school environment.

India is using Information and Communication Technologies (ICT) to leapfrog economic development in key sectors: health, education, infrastructure, finance, agriculture, manufacturing, and governance. ICT is being used to deliver critical goods and services to hundreds of millions of Indian citizens. While many sectors have already seen huge improvements through innovative use of ICT, such as infrastructure and communications, the education sector has struggled to optimize the potential of ICT for improving teaching and learning. ICT holds an important promise for education especially in rural areas, if it is optimized and tailored to local needs.

Today, the implementation of new technologies (ICT) has challenged the traditional method and process of teaching and learning and have also change the way of education is managed to a more flexible, user friendly and simplified form. The United Nation Education Scientific and Cultural Organizations (UNESCO, 2004) focuses that ICT has turned from being a technology of communication and information alone, but to a curriculum creation and delivery system for educator and learners.

According to Obanya (2002), ICT has to do with utilization of process, the methods and the product of electronic communication related technologies and other related resources in todays knowledge driven society, for enhancing the productivity, the spread and efficiency of set programme activities feared towards the achievement of clearly defined goals. In the world, ICT and IT (Information Technology) are often used synonymously. However, the key difference is that IT is a subset of ICT which covers all forms of communication including telephone, mobiles etc while information technology (IT) refers to an entire industry that uses computers, networking, software and all other equipment to manage information.

According to United Nation Educational Scientific and Cultural Organization (UNESCO, 2005), ICT is defined as the combination of all the computers, telecommunication and media technologies. They also used these electronic technologies for accessing, processing, gathering, manipulating and presenting or communicating information in education system.

Edozie et al. (2010) stated that Information and Communication Technologies (ICTs) self-

responsibilities enhances the abilities of people to use ICT to improve their life skills and strengthen their capabilities Such responsibilities could be facilitated awareness and motivation for ICTs. With this regards of their view, Umunadi (2011) added that the role of information and communication technologies in teaching and learning is rapidly becoming one of the most important widely discussed issues in secondary school in Nigeria. In another view, Openion of Obanya (2009) expressed that secondary school in Nigeria must strive to meet common 21st century challenges of providing student with an education that is viewed by the general society as relevant and valuable, and that teaching and learning must be driven by ICTs for effectiveness.

As per United Nation Educational Scientific and Cultural Organization (UNESCO, 2005), ICT is defined as the combination of all the computers, telecommunication and media technologies. In education system, ICT is electronic technology used for accessing, processing, gathering, manipulating and presenting or communicating information.

According to Maharashtra Digital School Survey Finding Report (2020), Maharashtra State has prioritized the integration of technology in teaching practice as a key area for helping to raise learning outcomes for students across the state. In order to guide their investments, the state is interested in identifying the most effective tools and approaches for various types of learning environments within the state that can be scaled up.

This paper focuses on Information and Communication Technology (ICT) is defined as electronic media, devices and application used in the classroom to and effective teaching and learning processes. All such materials, media and devices provided by ICT which appeal to all the senses and feeling and learning constitute teaching and learning materials. The materials help teachers communicate effectively to the students so that learning is facilitated. The development of ICT into the school's system will have effect upon the technological revolution expected in business and economic environment and the global society.

Statement of Problem:

The problem of the study stated as: Does ICT enhance effectiveness by secondary school teachers in teaching and learning? This is the problem to be investigated by this study.

Purpose of the study:

The main purpose of this study is to examine information and communication technology effectively used in secondary school teachers in Pune District area of Maharashtra State.

Specifically, the aim of the study is to:

- Investigate the extent of utilization of ICT tools by Teachers in secondary schools in Pune district area of Maharashtra State.
- Examine the use of ICT tools in evaluating teaching and learning process by Teachers of

secondary schools in Pune district area of Maharashtra State.

- Describe the constraints of effective utilization of ICT by Teachers in Pune district area of Maharashtra State.

Research Questions:

- To What extent are ICT tools used and utilized by school Teachersof secondary schools in Pune district area of Maharashtra State?
- How are ICT tools use in evaluating teaching and learning process by school Teachersof secondary schools in Pune district area of Maharashtra State?
- What are the constraints to effective utilization of ICT by school Teachers of secondary schools in Pune district area of Maharashtra State?

2. Methodology:

Researcher used a descriptive survey to carry out the study. This is because it has beneficial for permitting description of conditions as they exist in their natural setting. This survey research is a kind of research which involves the assessment of all school related public opinion using questionnaire. So, this study specifies to obtain information from teacherson the use of effectiveness of ICT in teaching and learning. This research work was carried out in Pune District of Maharashtra state. Researcher physically visited each selected school, distribute the questionnaire and after giving some duration collect the data for analysis. The populationof the study consisted of different regions secondary schools' teachers of fifty-nine (59) selected secondary schools of Pune District, Maharashtra State. The sample size of study was two hundred thirty-six (236) teachers of the schools' respondents. For the sample selection, researcher adopt aSimple random sampling technique for this study. Researcher use the questionnaire, this was considered necessary for the collection of data for the study because it has the characteristic of being used to ascertain facts, opinions, beliefs, attitudes and practices of the respondents. The respondents' responses in the questionnaire items were used to analyze the research questions.

After collecting the data from the respondents, researcher specify the code to the answer as per each question ask to respondent like Yes, No, Agree, Disagree, Satisfied etc. Researcher use the Microsoft Excel to store the raw data. This data prepared and coded as per the statistical method using questionnaire. For this analysis researcher used Microsoft Excel, R and R Studio 4.2.1 software as a tool and through this tool researcher get the summary of data and describe the data in tabular and tree structured format using evolutionary algorithms like decision and classification tree, regression and classification methods, recursive partitioning i.e. CART method etc.

The study attempts to fit a classification, recursive partitioning and regression trees i.e. CART method. "The decision tree method is a powerful and popular predictive machine learning

technique that is used for both classification and regression" [1]. This method known as Classification and Regression Tree (CART)[2].Also, researcher use a Chi-Square statically analysis was done to find the difference between area wise data from the schools.

The R implementation is carried out for this study, this implementation of the CART algorithm is called RPART (Recursive Partitioning and Regression Trees). "Here researcher use R software coding to compute and process classification and regression trees."

Data Analysis:

As per research question specified above, researcher explain the data analysis, data presentation using the different computational tools and statistical methods specified earlier.

Here, researcher collect the data from Pune District different region on whether the teachers utilize the ICT tools for different school activity's purpose or not? i.e., to what extent ICT tools utilized by the teachers of a school? Following table shows the data received from the respondent.

Area -→ Purpose |	**Baramati**		**Bhor**		**Daund**		**Indapur**		**Jejuri**		**Junner**		**Nira**		**Pune City**		**Saswad**	
Response	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N
Tools Use Everyday	24	24	13	7	13	11	27	13	14	6	9	3	9	3	32	8	11	9
Maintain School Records	31	17	17	3	22	2	33	7	16	4	10	2	11	1	35	5	13	7
Software for typing	44	4	17	3	24	0	33	7	17	3	11	1	12	0	31	9	19	1
Excel to Prepare Result	48	0	17	3	22	2	31	9	16	4	11	1	11	1	30	0	20	0
PPT in teaching	44	4	17	3	24	0	33	7	17	3	11	1	12	0	31	9	19	1
Operate Printer	37	11	17	3	23	1	31	9	16	4	10	2	11	1	25	9	19	1
Internet & Search educational Material	48	0	17	3	24	0	35	5	17	3	11	1	12	0	30	0	20	0
Have email account?	44	4	20	0	24	0	40	0	20	0	12	0	12	0	31	9	19	1
Computer / Laptop in Teaching	46	2	20	0	21	3	30	10	19	1	12	0	11	1	30	0	20	0
Comfortable using computer	48	0	20	0	24	0	30	0	20	0	12	0	12	0	30	0	20	0

Table 1: Utilization of ICT tools by Teachers of a school.

Above table shows almost in all regions utilization of ICT tools by teachers specified in the questions. As per the data collected its percentage is near about 80-85% utilized these tools by the school teachers.

Here researcher find and presentbelow the tree structured format summary of the Table 1 data and describe the data through classification and regression tree methodology (Recursive Partitioning Method)(CART), it is evolutionary algorithm method used with the objective of creating a model that predicts the value of target (or dependent variable) based on the values of several input (or independent variable), through this researcher find the RPART. Here researcher uses questionnaire for collecting data contains question number 38 to 47 for the opinion questions, so the Q30 to Q47 appear in tree structure. This processed data as follows:

n= 236 node), split, n, loss, yval, (yprob) * denotes terminal node

1) root 236 188 Baramati (0.2 0.085 0.1 0.17 0.085 0.051 0.051 0.17 0.085)

2) Q45=1 222 178 Baramati (0.2 0.09 0.11 0.18 0.09 0.054 0.054 0.14 0.086)

4) Q46=0 17 7 Indapur (0.12 0 0.18 0.59 0.059 0 0.059 0 0) *

5) Q46=1 205 163 Baramati (0.2 0.098 0.1 0.15 0.093 0.059 0.054 0.15 0.093)

10) Q39=0 44 27 Baramati (0.39 0.068 0.045 0.068 0.091 0.045 0.023 0.11 0.16)

20) Q40=0 8 5 Bhor (0 0.38 0 0.12 0.38 0.12 0 0 0) *

21) Q40=1 36 19 Baramati (0.47 0 0.056 0.056 0.028 0.028 0.028 0.14 0.19) *

11) Q39=1 161 134 Indapur(0.16 0.11 0.12 0.17 0.093 0.062 0.062 0.160.075)

22) Q43=1 148 123 Indapur(0.14 0.11 0.12 0.17 0.1 0.068 0.068 0.14 0.081)*

23) Q43=0 13 7 Pune City (0.31 0 0.077 0.15 0 0 0 0.46 0) *

3) Q45=0 14 5 Pune City (0.29 0 0 0 0 0 0 0.64 0.071) *

Now here researcher represents the above R coding result data in tree structure and partitioning it with the help of CART method and specifies the defining features as:

Response Variable: Area Method: CART

Variables used for partitioning: Q38 to Q47

Number of Partition sets: 06

Terminal Leaf Node	**No. of Responses (n values)**	**Label**	**Defining features**
3:	14	Pune City	Q45 = 0
23:	13	Pune City	Q43 = 0 Q39 = 1 Q46 = 1 Q45 = 1
22:	148	Indapur	Q43 = 1 Q39 = 1 Q46 = 1 Q45 = 1
21:	36	Baramati	Q40 = 1 Q39 = 0 Q46 = 1 Q45 = 1
20:	8	Bhor	Q40 = 0 Q39 = 0 Q46 = 1 Q45 = 1

4:	17	Indapur	Q46 = 0

Variable Importance:

Q40	Q45	Q46	Q39	Q43	Q41	Q42	Q38	Q44
22	21	20	14	10	4	4	3	3

Above data shows that in Baramati school teachers uses ICT for software for typing documents, also uses their email account, uses computer / laptop in teaching but not used to maintain school records. In Indapur, maximum teachers use ICT for maintain school records, operate printers, use email account and use computer / laptop in teaching. In Bhor, teachers not use ICT for maintain school records, also not used software for typing documents but they use an email account and uses computer / laptops in teaching. From the above data we get the tree as:

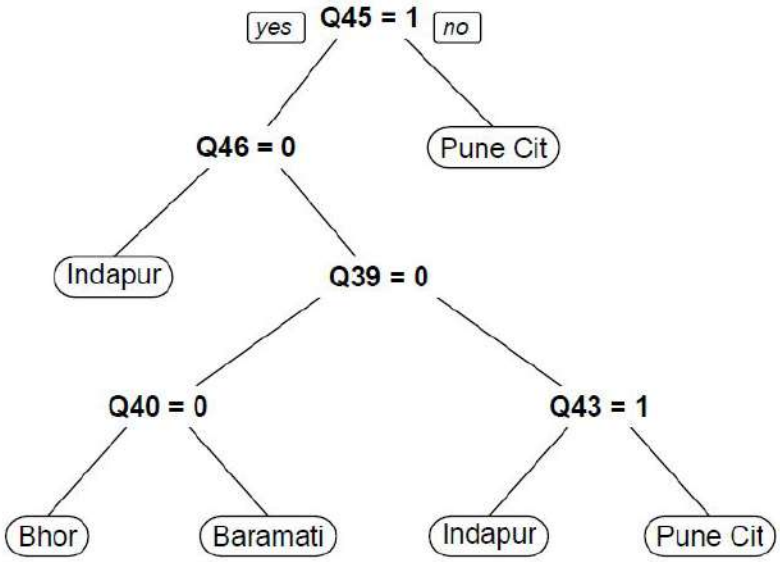

Fig: TT1: Teachers Data tree 1

Here researcher collected the data about whether the school evaluate teaching and learning process and promote to the teachers to use the ICT in teaching and learning in different ways. Following table shows the collected data.Here following table shows that to what extent teachers are confident in the ICT related skills? Responses we get in the form of a lot skill knows and used, sometimes i.e., partially used, a little time used and none i.e., not at all about use such skills in it. Means here researcher evaluate the ICT skills up to what extent teachers confident to use it.

Response → **Skills used by Teachers |**	**A lot (4)**	**Partially (3)**	**A little (2)**	**Not At All (1)**
Edit documents, multimedia, online links & images, online questionnaire, organize files and folders.	59	86	52	38

Create database, use spreadsheet and plot graphs	71	73	55	37
Create a presentation with animations, video, audio	63	67	44	63
Use emails to communicate others, create and maintain blogs, websites.	82	54	30	70
Participate in social network	41	59	54	82
Install software, download & upload resources from website or learning platforms for students to use	54	86	48	49
Teach students how to behave safely and ethically online	96	63	53	26
Prepare materials to use with an interactive whiteboard	35	53	55	93

Table 2: Evaluation of ICT by Teacher at their teaching & learning

Above table shows that, ICT skills like edit document, use of skills to prepare spreadsheet, presentations, use of mail, installation skills and download, upload skill and also get some resources from websites or learning platforms for students done by 60% to 70% teachers. Also, a lot of teachers give knowledge to students about safely land ethically behavior when they work online. Less number of teachers use the interactive whiteboard for prepare the material.

Researcher find, processed and represented the above evaluation based data in tree structure using classification and regression tree and some statistical methods. This tree structure describe and indicated that the teachers skill related to ICT, means teacher is confident about the implementation of different ICT work at its own. The skills are:

- Edit and create documents, databases, spreadsheets and presentations with features, organize files and folders.
- Use email to communicate others i.e., administration, students, parents etc., create and maintain blogs, websites and online activities.
- Install different software, download & upload resources from the website or learning platforms for students to use and teach the work safely and ethically online.

Researcher find the tree structure with coding and classification as:

n= 236 node), split, n, loss, yval, (yprob) * denotes terminal node

1) root 236 188 Baramati (0.2 0.085 0.1 0.17 0.085 0.051 0.051 0.17 0.085)

2) Q62.01=1,2,3 137 105 Baramati (0.23 0.12 0.073 0.2 0.12 0.073 0.058 0 0.12)

4) Q62.01=3 65 41 Baramati (0.37 0.046 0.11 0.2 0.015 0.031 0.046 0 0.18)

8) Q62.14=1 28 10 Baramati (0.64 0 0.036 0.071 0 0 0 0 0.25) *

9) Q62.14=2,3,4 37 26 Indapur (0.16 0.081 0.16 0.3 0.027 0.054 0.081 0 0.14)

18) Q62.10=3 10 4 Baramati (0.6 0 0.3 0 0 0 0 0 0.1) *

19) Q62.10=2,4 27 16 Indapur (0 0.11 0.11 0.41 0.037 0.074 0.11 0 0.15)

38) Q62.07=1,3,4 15 6 Indapur (0 0.067 0.2 0.6 0.067 0 0.067 0 0) *

39) Q62.07=2 12 8 Saswad (0 0.17 0 0.17 0 0.17 0.17 0 0.33) *

5) Q62.01=1,2 72 57 Jejuri (0.11 0.19 0.042 0.19 0.21 0.11 0.069 0 0.069)

10) Q62.02=1,3,4 54 39 Jejuri (0.15 0.22 0.056 0.11 0.28 0.11 0.056 0 0.019)

20) Q62.18=1 16 11 Baramati (0.31 0 0.19 0.12 0.12 0.062 0.12 0 0.062) *

21) Q62.18=2,4 38 25 Jejuri (0.079 0.32 0 0.11 0.34 0.13 0.026 0 0) *

11) Q62.02=2 18 10 Indapur (0 0.11 0 0.44 0 0.11 0.11 0 0.22) *

3) Q62.01=4 99 59 Pune City (0.16 0.03 0.14 0.13 0.04 0.02 0.04 0.4 0.03)

6) Q62.08=4 55 42 Daund (0.11 0.055 0.24 0.2 0.073 0.036 0.073 0.2 0.018)

12) Q62.13=1,2 23 15 Daund (0 0.13 0.35 0.35 0.087 0 0.087 0 0) *

13) Q62.13=3,4 32 21 Pune City (0.19 0 0.16 0.094 0.062 0.062 0.062 0.34 0.031) *

7) Q62.08=2,3 44 15 Pune City (0.23 0 0.023 0.045 0 0 0 0.66 0.045) *

After get the earlier format data, researcher represents the result in tree structure and partitioning it with the help of CART method and specifies the defining features as:

Response Variable: Area Method: CART

Variables used for partitioning: Q62.01 to Q62.20 (rpart)

Number of Partition sets: 10

Terminal Leaf Node	**No. of Responses (n values)**	**Label**	**Defining features**
7:	44	Pune City	Q62.08 = 2, 3 Q62.01 = 4
13:	32	Pune City	Q62.13 = 3, 4 Q62.08 = 4 Q62.01 = 4
12:	23	Daund	Q62.13 = 1, 2 Q62.08 = 4 Q62.01 = 4
11:	18	Indapur	Q62.02 = 2 Q62.01 = 1, 2
21:	38	Jejuri	Q62.18 = 2, 4 Q62.02 = 1, 3, 4 Q62.01 = 1, 2
20:	16	Baramati	Q62.18 = 1 Q62.02 = 1, 3, 4 Q62.01 = 1, 2

39:	12	Saswad	Q62.07 = 2 Q62.10 = 2, 4 Q62.14 = 2, 3, 4 Q62.01 = 3
38:	15	Indapur	Q62.07 = 1, 3, 4 Q62.10 = 2, 4 Q62.14 = 2, 3, 4 Q62.01 = 3
18:	10	Baramati	Q62.10 = 3 Q62.14 = 2, 3, 4 Q62.01 = 3
8:	28	Baramati	Q62.14 = 1 Q62.01 = 3

Variable Importance:

Q62.14	Q62.11	Q62.1	Q62.15	Q62.10	Q62.07	Q62.16
10	10	9	8	7	6	5
Q62.13	Q62.20	Q62.12	Q62.08	Q62.02	Q62.17	Q62.18
5	5	5	5	4	3	3
Q62.09	Q62.03	Q62.04	Q62.06	Q62.19	Q62.05	
3	3	2	2	2	2	

After analyze the above data, pune city and daund teachers confident and Baramati region teachers little confident about the skill of editing different purpose documents. Email and online skills somewhat aware in Indapur, Jejuri, Saswad and Baramati region teachers but not confident about creating and maintaining blogs and websites. This data represented in tree format as:

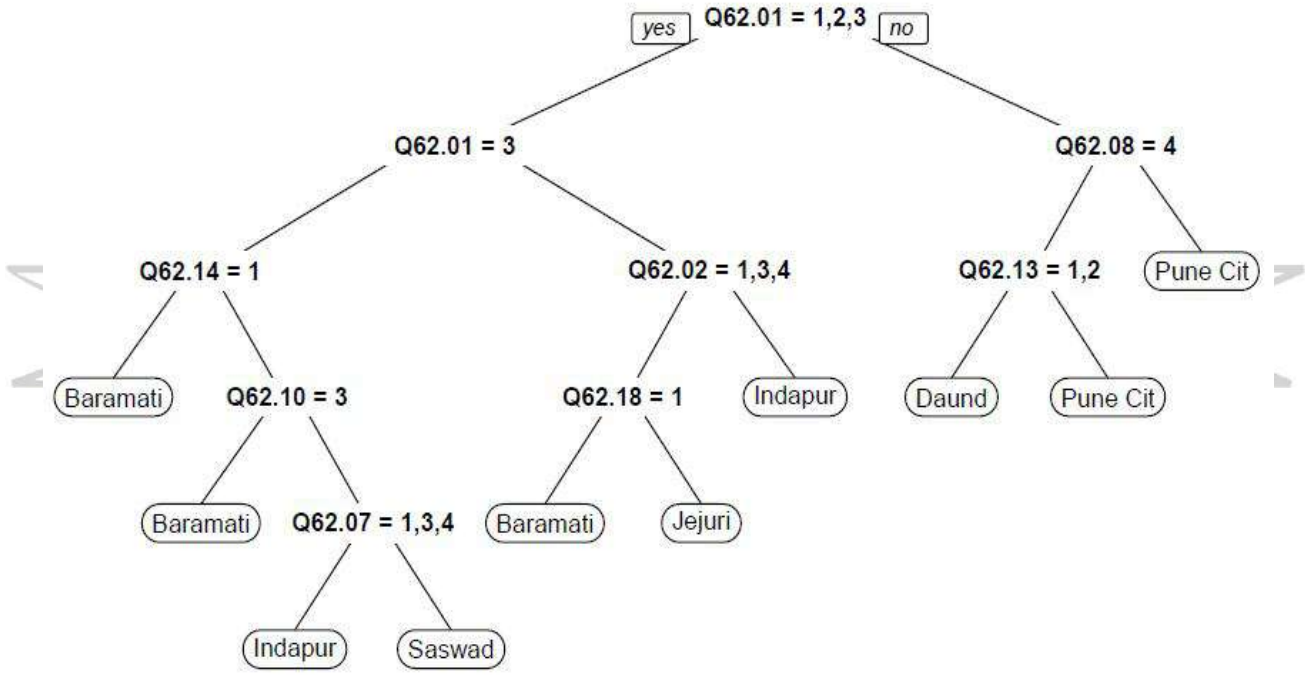

Fig. TT2: - Teachers Data Tree 2

As the third research question, what are the constraints to effective utilization of ICT by school teachers? Here researcher collected the data and specify the different constraints occurred during the ICT implementation in the school.Below table shows that different types of an obstacles give the major effect of implementing the ICT in teaching and learning.

Response → Obstacles by |	A lot (4)	Partially (3)	A little (2)	Not At All (1)
Insufficient number of computers	109	39	63	25
Insufficient number of internets connected computers	85	73	74	4
Insufficient internet bandwidth or speed	46	62	117	11
Insufficient number of interactive whiteboards	33	55	131	17
Insufficient number of Laptops/ notebooks	61	68	51	56
School computers out of date / need to repair	67	90	59	20
Lack of adequate skills of teachers	89	96	43	8
Insufficient pedagogical support for teachers.	75	70	66	25
Lack of adequate content/material for teaching	88	73	59	16
Too difficult to integrate ICT use into the curriculum	85	63	80	7
Lack of Pedagogical model on how to use ICT for learning	64	65	100	7
School time and space organization	75	110	32	30
Most parent not in favor of the use of ICT at school	104	86	26	20
Most teachers not in favor of the use of ICT at school	92	79	45	20
No or unclear benefit to use ICT for teaching	65	101	40	30

Table 3: Obstacles to using ICT in teaching and learning.

Through above table response says that a lot of obstacles occurred at the time of teaching and learning to the teachers, they are:

- Insufficient number of computers, internet connection.
- Most of parent and teacher not in favor of the use of ICT at school, also its difficult to

integrate ICT use into the curriculum, ICT is not benefited for teaching etc.

- Partially obstacles occurred by lack of adequate skills of teachers, school time and space for organization and no benefit to the school by sing ICT for teaching.
- A little obstacle occurred by insufficient internet bandwidth or speed, interactive whiteboards and lack of pedagogical model on how to use ICT for learning.

Above analysis of teachers obstacles represented in the tree structure using R coding and data tree occurred as:

n= 236 node), split, n, loss, yval, (yprob) * denotes terminal node

1) root 236 188 Baramati (0.2 0.085 0.1 0.17 0.085 0.051 0.051 0.17 0.085)

2) Q60.02=1,3,4 163 128 Baramati (0.21 0.12 0.11 0.17 0.1 0.055 0.055 0.055 0.11)

4) Q60.14=4 14 4 Indapur (0 0 0.14 0.71 0.071 0 0.071 0 0) *

5) Q60.14=1,2,3 149 114 Baramati (0.23 0.13 0.11 0.12 0.11 0.06 0.054 0.06 0.12)

10) Q60.08=1,4 64 37 Baramati (0.42 0.062 0.047 0.031 0.094 0.047 0.016 0.14 0.14)

20) Q60.04=1,2,4 33 12 Baramati (0.64 0 0.061 0 0.03 0.03 0.03 0 0.21) *

21) Q60.04=3 31 22 Pune City (0.19 0.13 0.032 0.065 0.16 0.065 0 0.29 0.065)

42) Q60.01=1 13 8 Jejuri (0 0.31 0 0.15 0.38 0.15 0 0 0) *

43) Q60.01=3 18 9 Pune City (0.33 0 0.056 0 0 0 0 0.5 0.11) *

11) Q60.08=2,3 85 69 Bhor (0.094 0.19 0.15 0.19 0.12 0.071 0.082 0 0.11)

22) Q60.17=1,3 49 37 Bhor (0 0.24 0.2 0.24 0.2 0.041 0.061 0 0)

44) Q60.20=1,2 28 17 Bhor (0 0.39 0.11 0.18 0.25 0.071 0 0 0) *

45) Q60.20=3 21 14 Daund (0 0.048 0.33 0.33 0.14 0 0.14 0 0) *

23) Q60.17=2 36 27 Saswad (0.22 0.11 0.083 0.11 0 0.11 0.11 0 0.25)

46) Q60.20=1,3 12 4 Baramati (0.67 0 0.25 0 0 0 0 0 0.083) *

47) Q60.20=2 24 16 Saswad (0 0.17 0 0.17 0 0.17 0.17 0 0.33) *

3) Q60.02=2 73 42 Pune City (0.18 0 0.082 0.16 0.041 0.041 0.041 0.42 0.027)

6) Q60.11=2 8 0 Indapur (0 0 0 1 0 0 0 0 0) *

7) Q60.11=1,3,4 65 34 Pune City (0.2 0 0.092 0.062 0.046 0.046 0.046 0.48 0.031) *

Here researcher represents the above R coding result data in tree structure and partitioning it with the help of CART method and specifies the defining features as:

Response Variable: Area Method: CART

Variables used for partitioning: Q60.01 to Q60.21 (rpart)

Number of Partition sets: 10

Terminal Leaf Node	**No. of Responses (n values)**	**Label**	**Defining features**
7:	65	Pune City	Q60.11 = 1, 3, 4 Q60.02 = 2

6:	8	Indapur	Q60.11 = 2 Q60.02 = 2
47:	24	Saswad	Q60.20 = 2 Q60.17 = 2 Q60.08 = 2, 3 Q60.14 = 1, 2, 3 Q60.02 = 1, 3, 4
46:	12	Baramati	Q60.20 = 1, 3 Q60.17 = 2 Q60.08 = 2, 3 Q60.14 = 1, 2, 3 Q60.02 = 1, 3, 4
45:	21	Daund	Q60.20 = 3 Q60.17 = 1, 3 Q60.08 = 2, 3 Q60.14 = 1, 2, 3 Q60.02 = 1, 3, 4
44:	28	Bhor	Q60.20 = 1, 2 Q60.17 = 1, 3 Q60.08 = 2, 3 Q60.14 = 1, 2, 3 Q60.02 = 1, 3, 4
43:	18	Pune City	Q60.01 = 3 Q60.04 = 3 Q60.08 = 1, 4 Q60.14 = 1, 2, 3 Q60.02 = 1, 3, 4
42:	13	Jejuri	Q60.01 = 1 Q60.04 = 3 Q60.08 = 1, 4 Q60.14 = 1, 2, 3 Q60.02 = 1, 3, 4
20:	33	Baramati	Q60.04 = 1, 2, 4 Q60.08 = 1, 4 Q60.14 = 1, 2, 3 Q60.02 = 1, 3, 4
4:	14	Indapur	Q60.14 = 4 Q60.02 = 1, 3, 4

Variable Importance:

Q60.20	Q60.01	Q60.14	Q60.02	Q60.11	Q60.04	Q60.12
10	9	9	8	8	7	7
Q60.03	Q60.08	Q60.18	Q60.17	Q60.09	Q60.05	Q60.07
5	4	4	4	4	3	3
Q60.13	Q60.06	Q60.21	Q60.16	Q60.15	Q60.10	
3	3	3	2	2	2	

Above response state that, above mentioned obstacles occurred in teaching and learning in different school area in the district at teachers point of view.

It describes as:

- Pune city and Indapur schools have an obstacle of lack of adequate contents/material for teaching.

- In Baramati, Saswad, Daund and Bhor schools have an obstacle of no benefit to use of ICT for teaching.
- In Jejuri, Pune city have an obstacle of insufficient of computers, also in baramati have an obstacle of insufficient number of interactive white board. School space and storage have an obstacle in Indapur schools.

This data represented in tree structure as follows.

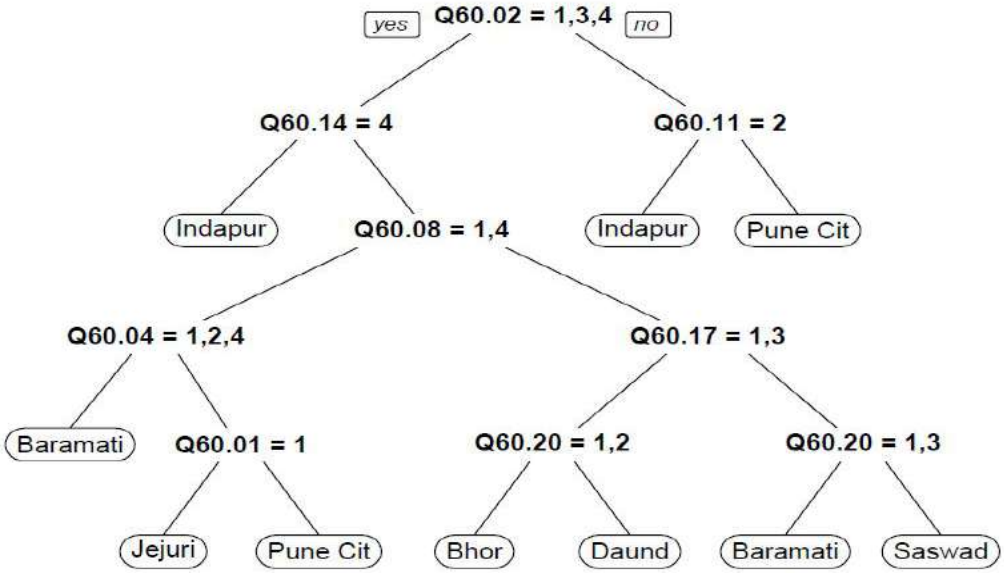

Fig.TT3: – Teachers Data Tree 3

References:

1. Agboeze, M. U.,Ugwoke, E. O. &Onu, F. M. (2012). Utilization of e-learning technology resources in accounting education instructional delivery methods in Nigerian universities. International journal of education research, 12(1), 26-38.
2. An Effective use of ICT for Education and Learning by Drawing on Worldwide Knowledge, Research, and Experience: ICT as a Change Agent for Education (A LITERATURE REVIEW)
3. Syed Noor-Ul-Amin, Ph.D Research Scholar, Department Of Education, University Of Kashmir.
4. Barriers Perceived by Teachers for use of Information and Communication Technology (ICT) in the Classroom in Maharashtra, India Chandan Singhavi and PremaBasargekar, K. J. Somaiya Institute of Management Studies and Research, India
5. Bangkok, U. (2004). Integrating ICTs into Education. Retrieved May 12, 2007, from ICT in Education: http://www.unescobkk.org/index.php?id=1793
6. Becker, H. J. (2000). "Pedagogical Motivations for Student Computer Use that Leads to Student Engagement". Education Technology. **Vol.** 40, No. 5, Pp; 5-17.

7. Cholin, V. S. (2005).Study of the application of information technology for effective access to resources in Indian university libraries, The International Information & Library Review, vol. 37, no. 3, pp.189-197.
8. Daniels J.S. (2002) "Foreword" in Information and Communication Technology in Education–A Curriculum for Schools and Programme for Teacher Development. Paris: UNESCO.
9. Edozie, Chukwuma, G. Olibie, EyiucheInfeoma and Aghu, Ngozi, Nwabuge (2010). Evaluating
10. University student's awareness of information and communication technology. Empowerment in South-east zone of Nigeria for entrepreneurship development. Unizik Orient Journal of Education, 5(2), 31-40.
11. Obanya, P. A. (2009). Dreaming, living and doing education. Ibadan: Educational Research and Study Group.
12. Olelewe, C.J. & Amaka, E.U. (2011). Effective utilization of Information Communication Technology (ICT) for sustainable manpower development among computer educators in Colleges of education in South-East Geo-political zone of Nigeria, A paper presented at the 24th National Association of Technology Teachers (NATT) on Technical and Vocational Education Training (TVET) for Sustainable Industrial Development in Nigeria between 17th - 21st October at Umunze Federal College of Education, Anambra State.
13. Tara Stafford Ocansey and Anchal Sharma, (2020), Center for Sustainable Development, Earth Institute, Columbia University, Maharashtra Digital Schools Survey Finding Report, ICT India working papers #24.
14. Umunadi, E. K. (2011). Perception of technical education students on the role of ICT in general studies programme (GSP) in university education, International Journal of Academic Research in Business and Social Sciences, 1 (3), 190-206.
15. UNESCO Institute of Statistics, Guide to measuring information and communication Technologies (ICT) in Education. 2009. ISBN 978-92-9189-078-1 Ref: UIS/TD/09-04 http://www.uis.unesco.org
16. Watson, S. L., Watson W. R., (2011). The Role of Technology and Computer-Based Instruction in a Disadvantaged Alternative School's Culture of Learning, Computers in the Schools, vol. 28, no. 1, pp. 39-55.
17. http://www.stepwheel.in/jl0skr/could-not-find-function-tree-in-r.html
18. https://www.analyticssteps.com/blogs/classification-and-regression-tree-cart-algorithm.
19. https://scg.sdsu.edu/ctrees_r/