ISSN 2278-3091
Volume 9, No.4, July – August 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse92942020.pdf
https://doi.org/10.30534/ijatcse/2020/92942020

A Novel approach to Secure Patient Data in Cloud Storage

[1]A.Vikram, [2]Dr.Gopinath Ganapathy
[1]Research Scholar (FT),School of Computer Science and Engineering, Bharathidasan University, Tiruchirappalli. .
:vikramaug17081984@gmail.com
[2]Professor, School of Computer Science and Engineering, Bharathidasan University, Tiruchirappalli
gganapathy@gmail.com

ABSTRACT

Cloud Data's are vulnerable to malicious threats. Among the data that are stored in cloud, patient record stored by hospitals is profound to be sensitive. Security breaches are common in public cloud. In order to address this issue, a novel hybrid approach is provided in this paper. New round functions are introduced to increase the security level. To encrypt text data, stream cipher Chacha is utilized. Though Chacha cipher has been cryptanalyzed by many authors, still it is not feasible to attack this cipher in polynomial time. Next, to secure the scan images of the patients, two different encryption algorithms are utilized, namely, Advanced encryption standard (AES) and Blowfish. The encrypted data and images are finally stored in the cloud. It is observed that even if the adversary gets hold of the data, they cannot decipher to the original data in polynomial runtime.

Key words: Cloud, Round function, AES, Blowfish, Chacha

1 INTRODUCTION

Cloud is a data centre available over the internet and it relies on data sharing. Three major services are delivered by a cloud service provider and those consist of Infrastructure as a service (IaaS), Platform as a Service (PaaS) and Storage as a Service (SaaS). Many organizations avail cloud facility to store their data. Many hospital managements also prefer to store their sensitive data in public cloud by availing SaaS.

When data is stored in a public sharable environment, it always has a threat of being obscured. The author has described the significance of authentication and encryption in cloud computing structure in [1]. In order to address this issue efficiently, a novel hybrid approach is described in this work. To preserve text data, a stream cipher called Chacha is used. Chacha is a variant of Salsa20. It is a 256-bit cipher. A 6 round Chacha cipher was attacked with time complexity 2^{136} and the results are stated by Zhenqing et al. in [2]. Though the cipher is attackable, it is not actually feasible, thus making the cipher still secure. Also Chacha is a lightweight stream cipher which is cost efficient at both encryption and decryption.

The two algorithms employed to encrypt images are Advanced Encryption Standard (AES) and Blowfish. Both the algorithms are commonly used to secure an image. These algorithms are more suitable for image since they work in block oriented method. In [3], different image encryption techniques are analyzed. In [4], detailed description of image encryption and decryption using AES is given. Medien Zeghid et al., in [5] has given a modified AES based algorithm for image encryption. Irfan Landge et al., in [6] has projected a image encryption scheme using blowfish.

In [7], a hybrid cryptosystem for text and image files using Diffie-Hellman and blowfish techniques is proposed by Tapan Kumar hazra. A hybrid encryption technique that uses permutation of text and image based on hyperchaotic scheme is proposed in [8]. Smita et al., in [9] has described a hybrid encryption technique that makes use of DES and RSA for text data. Pia Singh, in [10] has given a method to encrypt and decrypt image using blowfish.

It could be observed that various techniques are available to encrypt and decrypt text and image efficiently. Also we could see that none of the techniques is tending towards addressing the security of both text and image or speech [11]. Motivated by this, we put forth a novel hybrid technique that can secure both text and image in a time and cost efficient way.

The following sections are organized as, proposed work in section 2, experiment and results in section 3 and conclusion in section 4.

2. PROPOSED WORK

The patient data is categorized as text and scan images. In this proposed work, text and scan images are handled separately. Section 2.1describes encryption technique and section 2.2 describes decryption technique.

2.1 Encryption

The text data in patient record is subjected to a round function. The output from the round function is fed as input to the lightweight stream cipher called Chacha. Its initial state includes 256 bit key, 128 bit constant, 64 bit nonce and 64 bit counter. Four parallel quarter round function make a round. We employ a 20 round Chacha. The quarter round of Chacha is given in Figure 1.

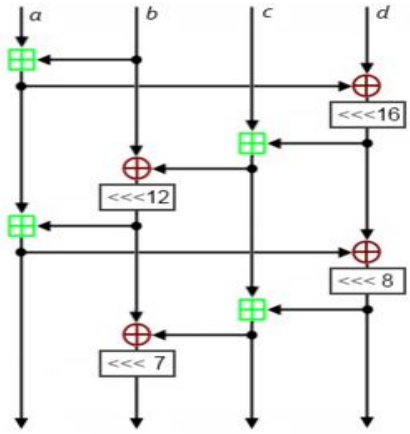


Figure 1: Quarter Round function of Chacha

The equation representation of quarter round of Chacha is represented as,

a+=b; d^=a; d<<<=16;
c+=d; b^=c; b<<<=12;
a+=b; d^a; d<<<=8;
c+=d; b^=c; b<<<7;

Next, the scan images are subjected to a round function. Followed by it, the output image is split into two blocks of equal size. Then, one block is encrypted with Advanced encryption Standard (AES) and the other is encrypted using Blowfish algorithm. A 14 round AES with 256-bit key is utilized in this work. AES contains four steps, namely, Substitute bytes, Shift rows, Mix columns and add round key. No proficient cryptanalysis has been so far proven against AES. The AES encryption and decryption are shown in Figure 2.

Blowfish is a block cipher and no predominant cryptanalysis has been proven against Blowfish. Since it is a block cipher, it works along well with image encryption. The block size of Blowfish is 64 bits. Its advantage is that it can have key size of varying length. We consider a 256 bit key size in our implementation for uniformity. The working function of Blowfish is given in Figure 3.

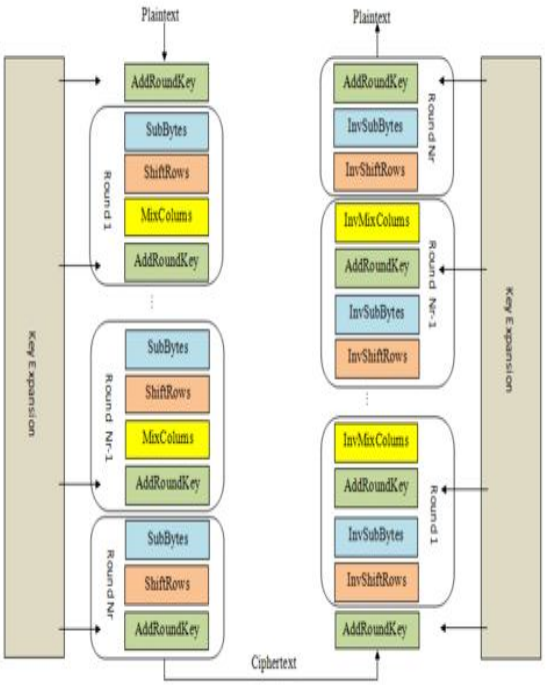


Figure 2: Encryption and Decryption of AES

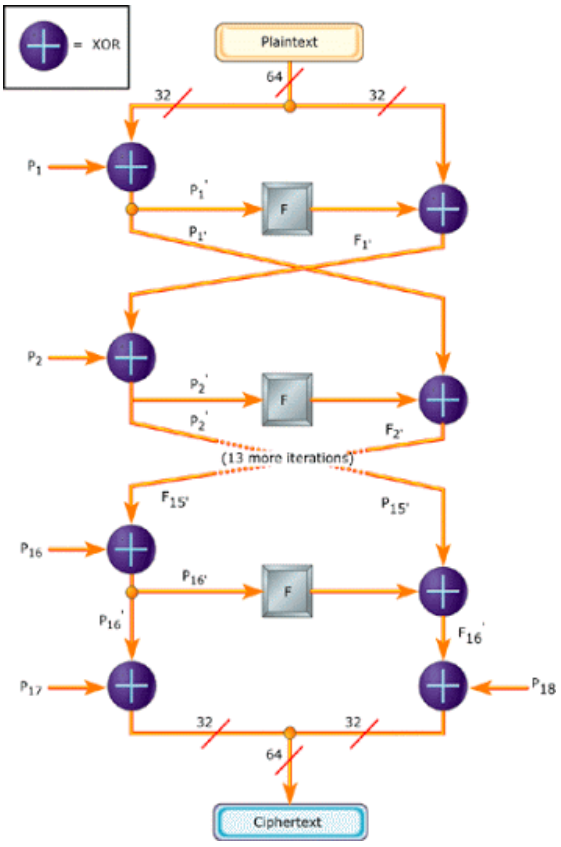


Figure 3: Working Principle of Blowfish

The encrypted text and image are thus stored in the public cloud. The architecture diagram of encryption methodology in the proposed work is given in Figure 4.

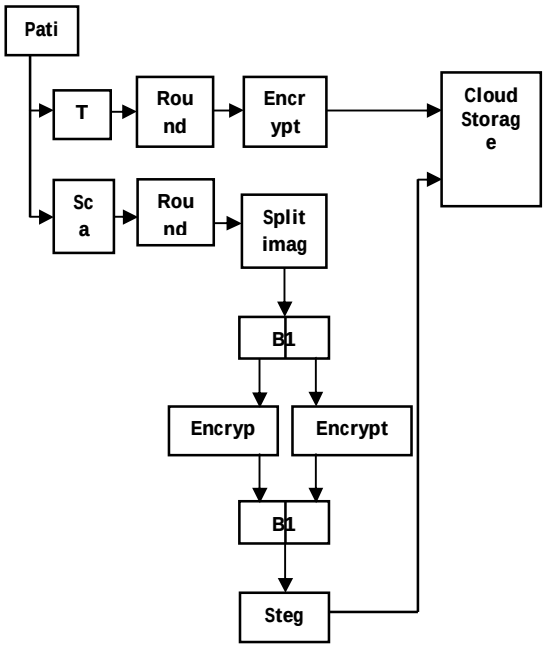


Figure 4: Encryption methodology

2.1.1 Round Function

The round function for text data is shown in Figure 5. The text data is split into two. Each half of the input text data is XORed with two different keys. The results are swapped and saved. This round function is performed ten times to increase randomness and security.

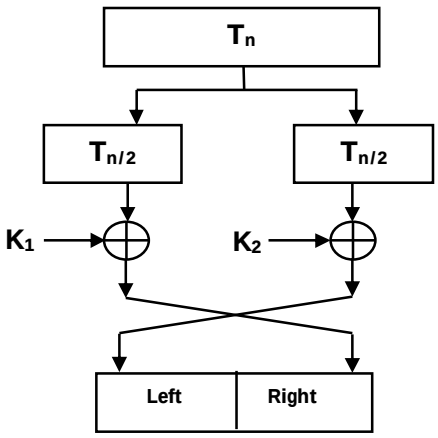


Figure 5: Round function for text data

The round function for scan images is shown in Figure .6. The image is split into two equal halves. Each half of the image is XORed with two different keys. The results are swapped and now we obtain new block 1 and new block 2. These blocks are then merged to obtain the output image. The rounds are repeated five times. Number of rounds for image is half of the number of rounds for text since image processing causes more overhead than text. In order to have a fast pre-processing phase, we restrict the number of rounds to be five for images.

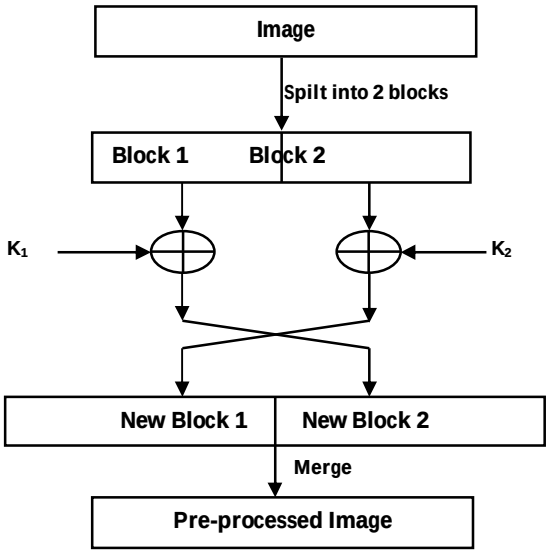


Figure .6. Function for scan images

2.2 Decryption

On retrieving the encrypted text data and scan image, they are decrypted separately. The encrypted text data is decrypted using Chacha. The output is subjected to inverse round function to obtain the original text data. In case of image, the stego image is split into two equal blocks. The blocks are decrypted using AES and Blowfish correspondingly. Then the blocks are merged. To the merged image, inverse round function is applied to obtain the original image. The architecture diagram of decryption process is given in Figure.7.

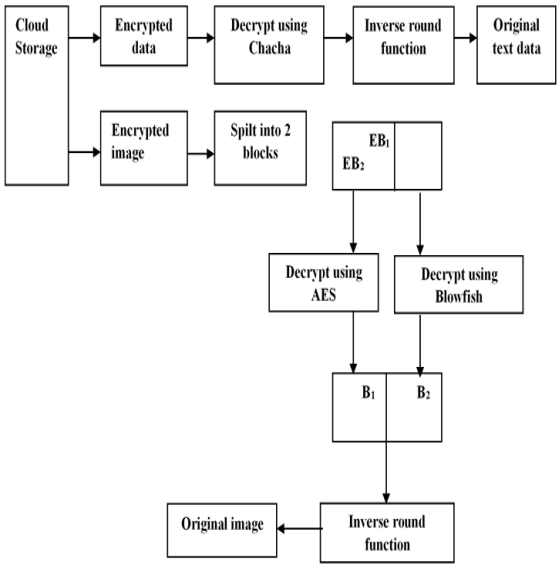


Figure 7: Decryption methodology

2.2.1 Inverse Round function

The inverse round function for text data in decryption process first splits the data into two equal halves and is the swapped. Keys are XORed with the halves. Then the data is merged to obtain the output text. The process is illustrated in Figure 8.

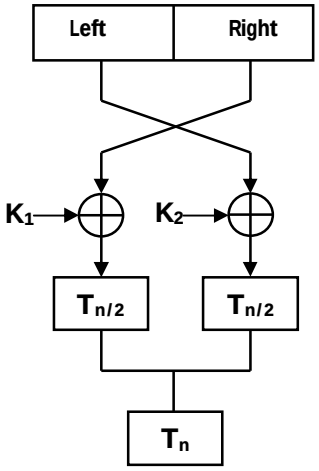


Figure 8: Inverse Round function for text data

The inverse round function for image splits the image into two equal sized blocks and then swaps them. Then keys are XORed. The blocks are then merged to obtain the output image. This process is illustrated in Figure 9.

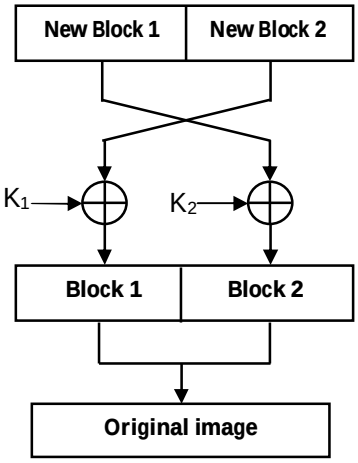


Figure 9: Inverse Round function for image

3 EXPERIMENTS AND RESULT

The introduction of round function in this method is to comparatively increase the security of the scheme. The key sizes are chosen based on the size of the text in case of text data and based on block size in case of image. The number of brute force attempts needed to break the round function is mentioned in table 1.

Table 1: Security of Round function

Key size	Number of brute force attempts needed	
	Text	Image
64 bits	10×2^{128}	5×2^{128}
128 bits	10×2^{256}	5×2^{256}
256 bits	10×2^{512}	5×2^{512}
512 bits	10×2^{1204}	5×2^{1024}

The encryption and decryption time for text data in the proposed method is given in table 2.

Table 2: Encryption and Decryption time for text data

Key size	Data size	Encryption time (in ms)	Decryption time (in ms)
32 bits	64 bits	51	52
32 bits	128 bits	53	54
32 bits	256 bits	58	57
32 bits	512 bits	63	62
64 bits	64 bits	55	53
64 bits	128 bits	59	59
64 bits	256 bits	64	63
64 bits	512 bits	66	67
128 bits	64 bits	68	66
128 bits	128 bits	73	74
128 bits	256 bits	74	76
128 bits	512 bits	78	79
256 bits	64 bits	75	74
256 bits	128 bits	80	79
256 bits	256 bits	82	83
256 bits	512 bits	83	84
512 bits	64 bits	86	85
512 bits	128 bits	89	88
512 bits	256 bits	93	92
512 bits	512 bits	97	96

The graphical plots of encryption and decryption times for text data are shown in figure 10.

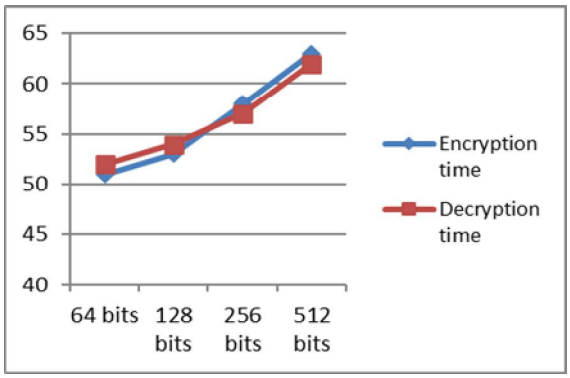


Figure 10 (a): Key size: 32 bits

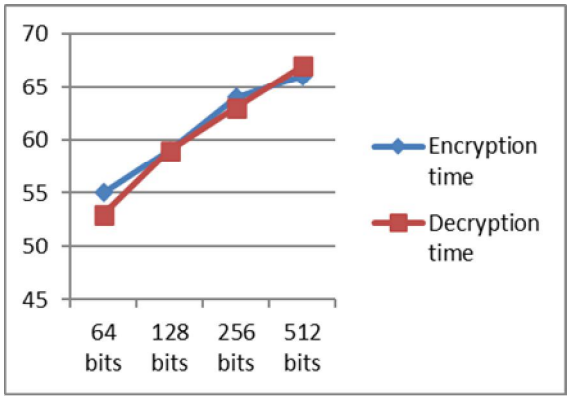


Figure 10 (b): Key size: 64 bits

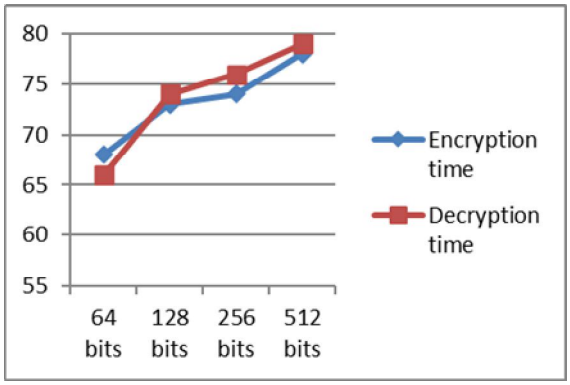


Figure 10 (c): Key size: 128 bits

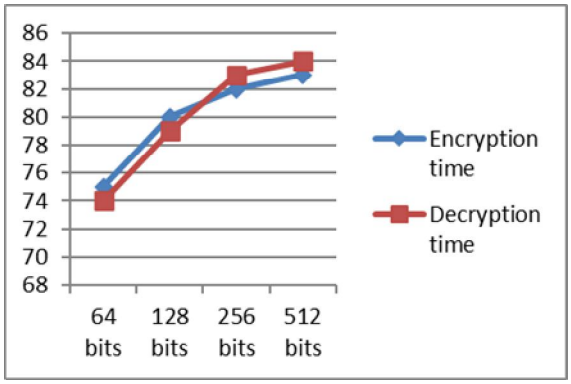


Figure 10 (d): Key size: 256 bits

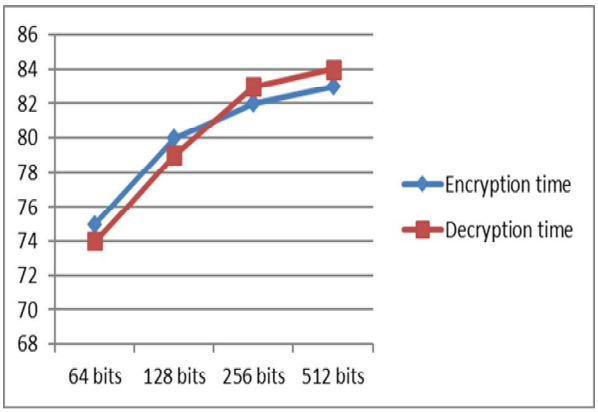


Figure 10 (e): Key size: 512 bits

The execution time for image in the proposed method is given in table 3.

Table 3: Encryption and Decryption times for image

Key size	Block size	Encryption time (in ms)	Decryption time (in ms)
32 bits	64 bits	84	86
32 bits	128 bits	89	88
32 bits	256 bits	94	96
32 bits	512 bits	96	97
64 bits	64 bits	89	90
64 bits	128 bits	93	94
64 bits	256 bits	99	98
64 bits	512 bits	102	101
128 bits	64 bits	95	97
128 bits	128 bits	97	99
128 bits	256 bits	100	101
128 bits	512 bits	104	102
256 bits	64 bits	101	100
256 bits	128 bits	106	105
256 bits	256 bits	111	110
256 bits	512 bits	118	119
512 bits	64 bits	107	106
512 bits	128 bits	119	117
512 bits	256 bits	134	132
512 bits	512 bits	145	147

The graphical plots of encryption and decryption times for text data are shown in figure 11.

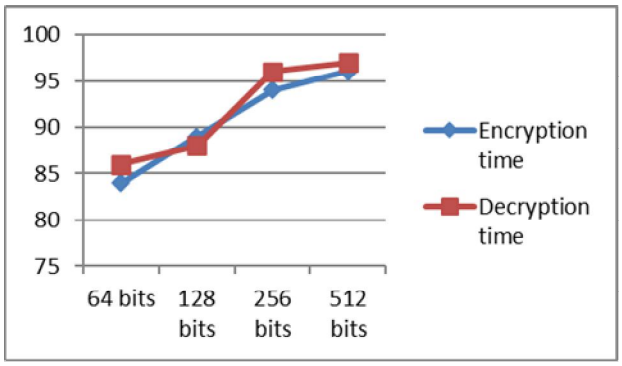


Figure 11 (a): Key size: 32 bits

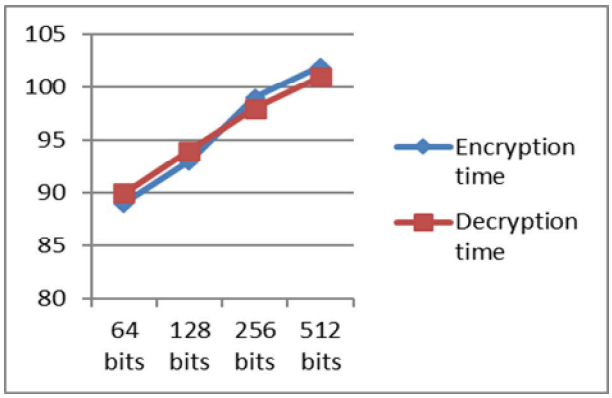


Figure 11 (b): Key size: 64 bits

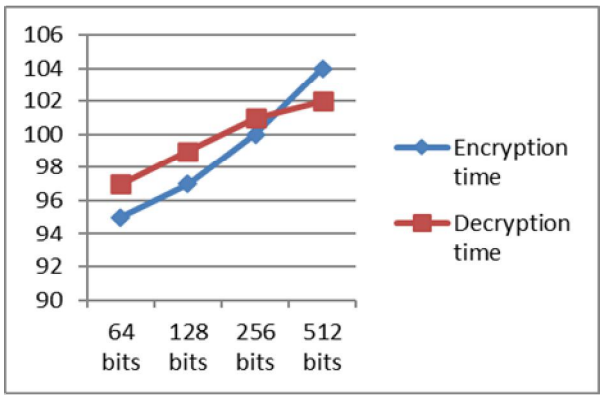


Figure 11 (c): Key size: 128 bits

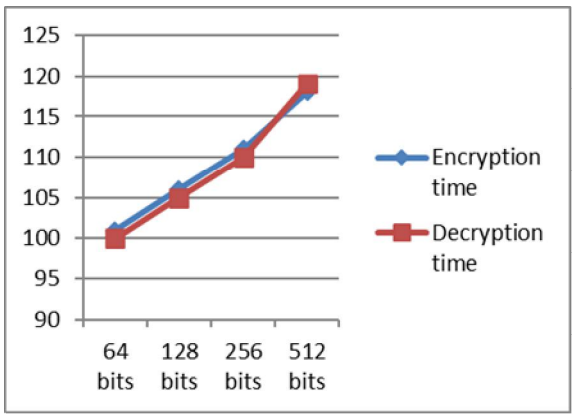


Figure 11 (d): Key size: 256 bits

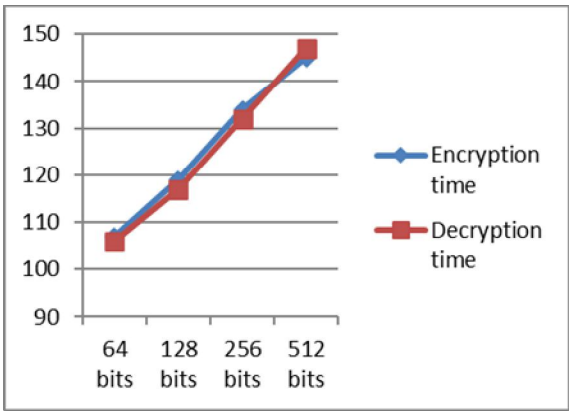
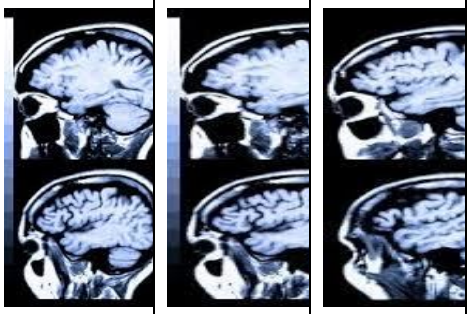
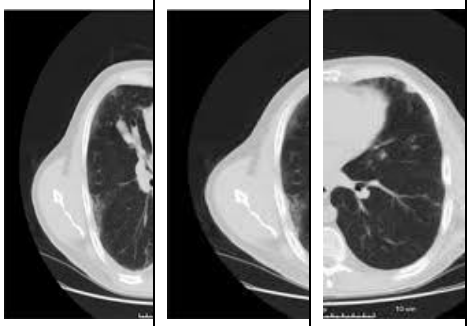
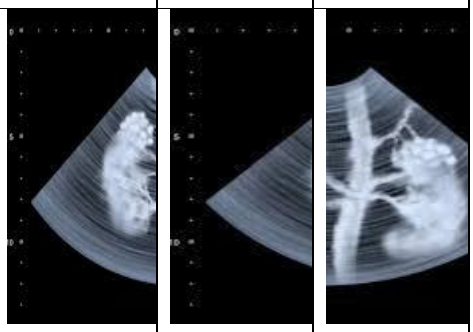


Figure 11 (e): Key size: 512 bits

The scan images taken for experiment and its split images are shown in table 4.

Table 4: Scan images and split images

Image name	Original Image	Sub image1	Sub image2
Head			
Chest			
Kidney			
Fetus			

			
Xray			

4. CONCLUSION

A lot of research works are being carried out for data security in cloud and various solutions have been provided to secure sensitive data like patients records. But it could be observed that there is not an efficient method to resolve all the issues in cloud data security. In order to address this issue, a novel hybrid approach is defined in this work to secure patient text data and scan images. To add novelty to the method, round functions are introduced which improve the security. Although round functions are added with the existing encryption algorithms, it could be seen from the experimental part that there is no significant overhead in execution time for encryption and decryption. Thus the methodology introduced in this work deems to provide high security with less runtime overhead.

REFERENCES

[1]. Jalgaonkar M, Kanojia **A. Adoption of cloud computing in distance learning.** International Journal of Advanced Trends in Computer Science and Engineering. No. 2, vol. 1, pp.17-20, 2013.

[2]. Zhenqing Shi, Bin Zhang, Dengguo Feng and Wenling Wu, **"Improved key recovery attacks on Reduced-Round Salsa20 and Chacha"**, *Springer, ICISC 2012, LNCS* vol. 78, no. 39, pp. 337-351, 2013. https://doi.org/10.1007/978-3-642-37682-5_24

[3]. Mohit Kumar, Akshat Aggarwal, Ankit Garg, "**A review on various digital image encryption techniques and security criteria**", *International Journal of Computer Applications*, Vol. 96, no. 13, 2014, pp 19 – 26. https://doi.org/10.5120/16854-6720

[4]. Priya Deshmukh, **"An image encryption and decryption using AES algorithm",** *International journal of Scientific & Engineering research*, vol. 7, no. 2, pp. 210 – 213, 2016.

[5]. Medien Zeghid, Mohsen Machhout, Lazhar Khriji, Adel Baganne, Rached Tourki, **"A modified AES based algorithm for image encryption",** *International Journal of computer science and Engineering*, Vol. 1, no. 78, pp. 70 – 75, 2007.

[6]. Irfan Landge, Burhanuddin Contractor, Aamna Patel, Rozina Choudhary, **"Image encryption and decryption using blowfish algorithm",** *World Journal of Sience and technology*, Vol. 2, no. 3, pp. 151 – 156, 2012.

[7]. Tapan kumar Hazra, Anisha Mahato, Arghyadeep Mandal, Ajoy kumar chakraborthy, **"A hybrid cryptosystem of image and text files using blowfish and Diffie-Hellman techniques",** *8th Annual Industrial automation and Electromechanical Engineering Conference (IEMECON)*, vol.18, no. 28, pp. 137 – 141, 2017.

[8]. Seddik Hassene, Maalaoui Najm Eddine, **"A new hybrid encryption technique permuting text and image based on hyperchaotic system"**, *2nd International conference on Advanced Technologies for signal and Image processing (ATSIP)*, vol.16, pp. 63 – 68, 2016.

[9]. Smita Chourasia, Kedar Nath Singh, **"An efficient hybrid encryption technique based on DES and RSA for textual data",** *Information systems Design and Intelligent Applications*, vol. 23, no.78. pp. 73 – 80, 2016.

[10]. Pia Singh, Karamjeet Singh, **"Image encryption and decryption using Blowfish algorithm in MATLAB"**, *International Journal of Scientific and Engineering Research*, Volume 4, Issue 7, pp 150 – 154, 2013.

[11]. Donepudi Babitha, Jayasankar.T, Sriram V.P, Sudhakar S, Kolla Bhanu Prakash," **Speech Emotion Recognition using State-of-Art Learning Algorithms",** International Journal of Advanced Trends in Computer Science and Engineering, Vol. 9, No. 2, pp.1340-1345, 2020. https://doi.org/10.30534/ijatcse/2020/67922020