A Comparison Of Symmetric Key Encryption Algorithms In Secure Cloud Storage Using Ehrs

S. Shwetha –[1] , P. Banupriya [2] , M. Nanthini –[3], S. Vaishnavi –[4] , Dr. M. P. Revathi[5] , Mrs. G. Keerthana , AP [6]

[4]Final year students , Associate Professor [5]
Department of Computer Science and Engineering, J. J. College of Engineering and Technology, Trichy.
shwethanaidu230@gmail.com,banupriyap2020@gmail.com,abinanthini123@gmail.com, sgvaishu0101@gmail.com , jjcetrevathi.cse@gmail.com, Meenaloshini14@gmail.com

ABSTRACT

Cryptographic techniques are play crucial role when the users exchange information. Data confidentiality is in any research organization refers to protecting the privacy of an individual's data is actively involved in their respective of the research domains. Data breach can therefore be a big threat of any research organization. Hence, it's very much important to maintain the confidentiality of data. However, we provide the security for patient data like electronic health record stored in the secure cloud storage. In this paper we will analyze different data encryption techniques to compare the execution time with other existing encryption algorithms. Encryption technique should be time efficient. In this work we consider six encryption techniques: Blowfish, AES, DES, 3DES, RC4 and IDEA and two different types of EHRs content: text and image, Simulation shows that AES is time efficient than others. Comparing between symmetric key cryptography algorithms, AES take less time than the other encryption techniques.

Keywords: Confidentiality, Cryptographic, Electronic Health Records, Cloud Storage, Encryption, Decryption

I. INTRODUCTION

During recent years the telecommunication industry has made tremendous progress in their development of systems that offer more bandwidth to the end user. User shares their learning, observation and experience with their community using networks of computer. There are different types if EHRs information like text and images are shared for the users. When these information transmit in computer network, it faces a lot of security threats. So it is necessary to protect the EHRs from unauthorized user. The solution is encryption. There are several encryption techniques. Choice of encryption technique depends on strength of the mathematics behind the algorithm, encryption time and strength against the attack on that algorithm. The Encryption techniques can be classified into Symmetric and Asymmetric key algorithm. The symmetric-key algorithms are also called as single-key is used to encrypt the data and asymmetric algorithm uses two different keys like Public and Private key are used to execute the process of encryption and decryption.

The main limitations of cryptographic system arise when the attackers try to attack using the brute force approach. For example, if the users use a single key for a symmetric key algorithm, so the attacker can guess that a single key using the brute force approach then she / he can found the real message from encrypted message using that a key. So in a secure algorithm, which could constructed and used a key which is guessing is to hard. There are many algorithms implementation is too difficult in mathematically (i.e.) AES and Blowfish algorithms are easy to implements. The implementation of AES algorithm have a lot of cycles and steps such as- the Key Expansions for the constructing key using a Rijndael's key schedule, Initial Round, Rounds which have subBytes, ShiftRows, MixColumns and AddRounds, and Final Rounds.

In the blowfish algorithm have a more number of steps such as a expansion of Key and encryption of data and a have some of the sub steps. It takes more time while encrypted the large size files. So, the authors to find the suitable encryption technique and it takes is less time. In this work we consider six most used encryption algorithms: Blowfish, AES DES, IDEA, RC4 and 3DES. Six algorithms are symmetric for encryption and decryption we use two different types of EHRs data: text and image.

Literature Review

In early most of research works carried on comparison between symmetric algorithms . In DES, AES, RSA and Blowfish algorithms are compared on the basis of rounds block size, key size and encryption / decryption time and it has shown that, Blowfish is better than other algorithm. In , image files are encrypted using different size like Kb & MB and its compare them. In two algorithms: Blowfish, and RC4 are compared with the parameter of rounds block size, key size and encryption / decryption time. In "Comparative

Implementation of Cryptographic Algorithms on ARM Platform", the authors consider two algorithms AES and Blowfish and compare basis of algorithm.

CRYPTOGRAPHIC ALGORITHMS

This section provides information about the cryptographic algorithms used in this work.There are two general categories of cryptographic keys: symmetric key and asymmetric key systems. The symmetric key systems use a single key. The single key is used both to encrypt and decrypt the information. Both sides of the transmission need to keep the key in secret from. The security of the transmission will depend on how well the key is protected. The biggest difficulty with this approach, of course, is the distribution of the key. Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Most popular symmetric key algorithms are DES, Triple DES, AES, IDEA, IDEA, Blowfish etc.[1][2]. Each algorithm has own advantages and limitations. Since EHR contents take much storage than others. We consider algorithms AES, Blowfish, suitable for large file.

AES:

AES stands for Advanced Encryption Standard also known as "Rijndael". It is symmetric block cipher algorithm. In 2001 two Belgian cryptographers "Joan Daemen" and "Vincent Rijmen" first develop this algorithm at National Institute of Standards and Technology (NIST). It supports 128 bits fixed length block size and variable length key size of 128, 192 and 256 bits[9][20]. AES is based on a design principle known as substitution-permutation network. And AES operates on a 4x4 column-major order matrix of byte. The key size used for an AES cipher specifies the number of repetitions of transformation rounds. For 128-bit keys needed 10 cycles of repetitions, for 192-bit keys needed 12 cycles of repetitions and for 256-bit keys needed 14 cycles of repetitions. Each round has some specific operations like, SubBytes, ShiftRows, MixColumns and Add Round Key.

AES use four types of transformations: substitution, permutation, mixing and key adding. In substitution, mathematical calculation is use for transforming each byte individually and only one table is use for this; it has two different processes. First is Sub Bytes, this transformation is use in encryptions it and transformation operation.

Involves 16 independent byte to byte transformations and another is In SubBytes, which is use in decryption site, operation is opposite of SubBytes. In permutation, permutes the bytes; operations are:- ShiftRows- In here rows are shifted such as Row 0: no shift, Row 1: 1-byte shift, Row 2: 2-bytes shifts and so on; is used in encryption site. The opposite of ShiftRow is In ShiftRow, which is used in decryption site. Mixing: In here, changes the bytes and create four byte at a time taking four byte input; Mix Columns and In Mix Columns are two different operations of Mixing, both are use in column level mixing, first one is use in encryption site and another one is use in decryption site. The last transformation is key-adding; probably it is the most important one. In here, operation Add Round Key adds a round key word with each state column matrix.

Another important operation of AES is Key-Expansion. We know AES use three different key size 128-bits, 192-bits and 256-bits. AES use different method to construct different size of key.

Blowfish:

Blowfish is one of most used encryption algorithm. In 1993 “Bruce Schneier” designed this algorithm. It is symmetric block cipher algorithm takes variable length keyfrom 32 bits to 448 bits. It can encrypt block data of 64-bits at a time. It was the nice alternatives of DES or IDEA . Blowfish use a large number of subkeys, and these keys must be constructed before encryption and decryption. It uses 1832-bit P-arrays: P_1,P_2, ,P_{18} And four 32-bits Sboxes have 256 entries each:

S1,0,S1,1,…………………………...,S1,255

S2,0,S2,1, ... ,S2,255

S3,0,S3,1, ... ,S3,255

S4,0,S4,1, ... ,S4,255

Blowfish is a Feistel network consisting of 16 round. It can take 64-bit data as input at a time.

It uses a Feistel function F is as follows: Divide x_L into four eight-bit quarters: a, b, c, and d $F(x_L)$ =XOR $((S_{1,a} + S_{2,b} \bmod 2^{32})$, $S_{3,c})$ + $S_{4,d}$ mod $2^{32.}$ Sub-keys are calculated as:

- Firstly initialize the P-arrays then four S-boxes using hexadecimal digits of P.
- XOR P_1 with first 32-bits of key then XOR P_2 with second 32-bits of key, this process continue up to P_{18}.
- Encrypt all-zero string using previous two steps and replace P_1 and P_2 with the output of this step.
- Encrypt output of the previous step; replace P_3 and P_4 with the output of this step.
- Continue this process for replacing all the contents of P-arrays and then all four S-boxesin order,with the output of the continuous output of Blowfish algorithm.

DES:

It is a symmetric encryption algorithm. It has two inputs, plain texts and keys. The length of the plaintext and the keys are both 64 bits, and 56 of them are valid keys, and the remaining 8 bits are the parity bit. The following figure is flow of the schematic diagram of the DES algorithm.

The processing steps for plaintext are as follows:

- Step1 Enter the plaintext into groups according to the 64bits packet length, and then rearrange the 64bits data block P through the initial permutation IP matrix.

- Step2 Use the f function to perform 16 rounds of iterative transformation of P after the initial permutation IP matrix transformation, and each round of transformation needs to use a different subkey.
- Step3 The 16th round output has 64bits, which is a function of the input plaintext and the key. It produces a 64bits data block as the result of this group of encryption through the inverse initial replacement IP-1 effect of the initial replacement IP.
- The formula for the i-th round of encryption above process can be expressed as Lei = REi-1

3DES:

Triple DES (3DES) has been adopted as a temporary standard and is incorporated in several international standards. 3DES is known as Encrypt-Decrypt-Encrypt (EDE) and Triple DEA (3DEA). 3DES is the name now most often given one popular form of multiple DES applications. Most 3DES implementations use two security keys. If the total length of the two keys has 112 bits, then cryptanalysis requires triple computational efforts compared to DES with 56-bit key length. The resultant 3DES cipher text is much harder to break. 3DES is a more secure DES morphing. 3DES algorithm is the cumulative computing of the three times DES algorithm that is the process of Encryption - Decryption - re-encryption. In order to obtain higher security, three keys should be separate.

IDEA:

The block cipher IDEA operates with 64-bit plaintext and cipher text blocks and is controlled by a 128-bit key. The fundamental innovation in the design of this algorithm is the use of operations from three different algebraic groups. The substitution boxes and the associated table lookups used in the block ciphers available to-date have been completely avoided. The algorithm structure has been chosen such that, with the exception that different key sub-blocks are used, the encryption process is identical to the decryption process. The 64-bit plaintext block is partitioned into four 16-bit sub-blocks, since all the algebraic operations used in the encryption process operate on 16-bit numbers. Another process produces for each of the encryption rounds, six 16-bit key sub-blocks from the 128-bit key. Since a further four 16-bit key-sub-blocks are required for the subsequent output transformation, a total of 52 (= 8 x 6 + 4) different 16-bit subblocks have to be generated from the 128-bit key.

RC4:

The RC4 algorithm has two phases, key generation, and encryption. Key generation is the first step and the most difficult in this algorithm. The encryption key is used to generate a variable encryption that uses two arrays, state and keys, and the results of merging operations. This merger operation consists of swapping, modulo, and other formulas. Modulo operation is the process that produces the residual value of the shares. For example, 11 divided by 4 is 2 with the rest of division is 3, if 7 modulo 4, it will produce 3. The variable emerges from the encryption key generation process will be conducted with the plaintext to produce encrypted text.

EXPERIMENT ALANALYSIS

In our work, we develop a simulator using java programming language where all of implementations of the algorithms for EHRs text and image files are takes place. Using that simulator we measure the encryption time of the program for various input size, then analyze the performance of the algorithms. For our experiment we use two types of EHRs content like text and image. In simulation, 50 samples of text data are considered. File size of text data varies from 10KB to 1MB. We take 20 JPG images vary from 100 KB to 2.2 MB. In our simulation we use128-bits key size for all of algorithms.

In the table 1 represents the encryption time for different EHR text files. The different symmetric key encryption algorithms are used to encrypt and the time is calculated in ms. the encryption time values are tabulated, here the AES algorithm took less time than the other algorithm.

Table1: Encryption times for different EHR text files

Time (ms)	10 KB	50 KB	100 KB	200 KB	400 KB	600 KB	800 KB	1 MB
Blowfish	1	1	1	2	5	8	11	21
AES	0	0	1	1	2	2	3	3
DES	0	1	3	1	3	4	5	6
IDEA	1	1	5	3	9	7	13	20
RC4	0	1	1	2	3	4	4	5
3DES	1	1	4	6	7	9	13	20

The figure 1 shows that the encryption time for different EHR text files as plotted in different colors. Orange color indicates the AES encryption time is taken less time. Table 2 represents the encryption time for different EHR text files. The different symmetric key decryption algorithms are used to encrypt and the time is calculated in ms. the encryption time values are tabulated, here the AES algorithm took less time than the other algorithm. The figure 2 shows that the encryption time for different EHR text files as plotted in different colors. Orange color indicates the AES decryption time, it takes less time.

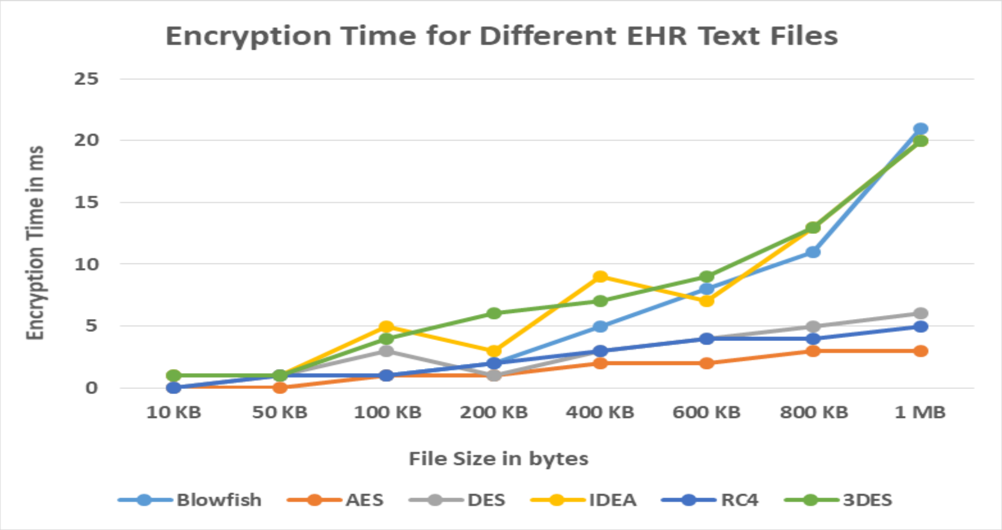

Figure 1: Encryption Time for Different EHR text files

Table 2: Decryption times for different text files

Time (ms)	10 KB	50 KB	100 KB	200 KB	400 KB	600 KB	800 KB	1 MB
Blowfish	1	1	2	3	6	14	16	22
AES	0	1	1	1	1	2	2	2
DES	0	1	1	2	3	4	4	4
IDEA	1	1	3	5	7	8	14	18
RC4	0	1	1	2	2	3	4	5
3DES	1	1	2	5	6	9	12	24

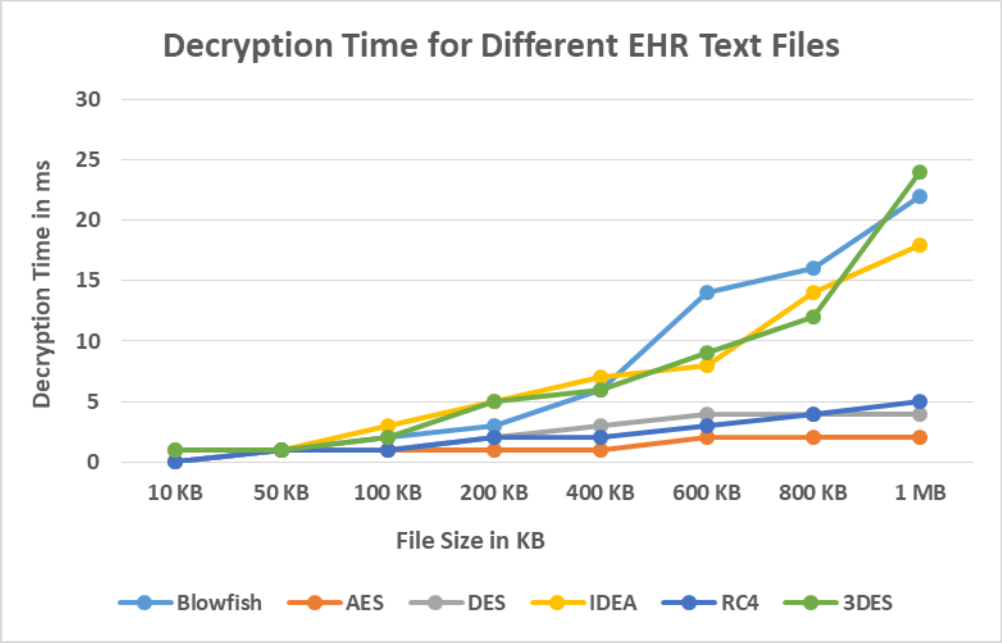

Figure 2: Decryption Time for Different EHR text files

The table 3 represents the encryption time for different EHR image files. The different symmetric key encryption algorithms are used to encrypt and the time is calculated in ms. the encryption time values are tabulated, here the AES algorithm took less time than the other algorithm. Figure 3 shows that the encryption time for different EHR image files as plotted in different colors. Orange color indicates the AES encryption time is taken less time. Table 4 represents the encryption time for different EHR text files. The different symmetric key decryption algorithms are used to encrypt and the time is calculated in ms. the encryption time values are tabulated, here the AES algorithm took less time than the other algorithm. Figure 4 shows that the encryption time for different EHR image files as plotted in different colors. Orange color indicates the AES decryption time, it takes less time.

Table 3: Encryption times for different image files

Time (ms)	100 KB	200 KB	500 KB	1000 KB	1200 KB	1500 KB	1800 KB	2.2 MB
Blowfish	2	3	6	15	16	22	24	33
AES	1	1	2	2	2	3	3	4
DES	1	2	3	4	4	5	5	6
IDEA	1	2	4	7	9	13	18	23
RC4	2	3	3	5	8	15	20	26
3DES	2	2	6	9	12	17	23	29

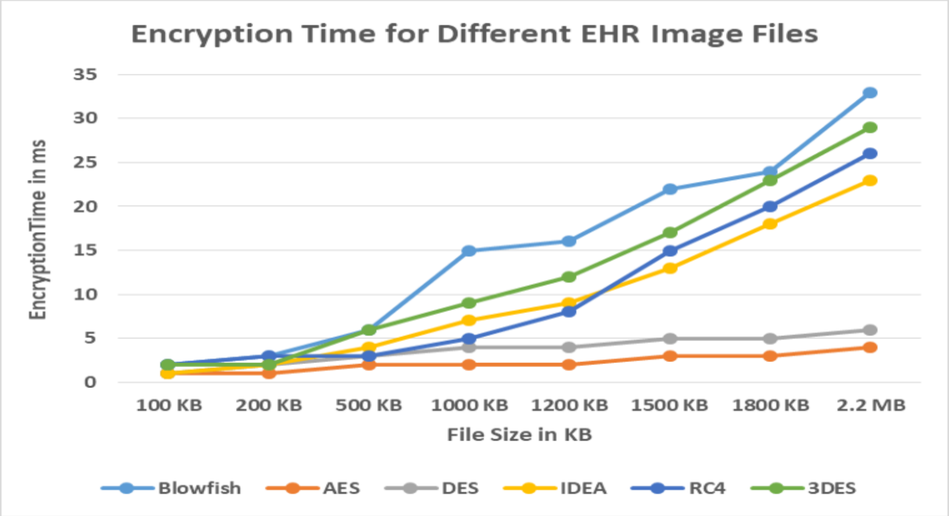

Figure 3: Encryption times for different image files

Table 4: Decryption times for different image files

Time (ms)	100 KB	200 KB	500 KB	1000 KB	1200 KB	1500 KB	1800 KB	2.2 MB
Blowfish	2	4	7	14	18	25	28	35
AES	1	2	2	3	3	3	4	4
DES	1	2	4	4	4	6	6	7

IDEA	2	4	7	7	10	15	19	28
RC4	2	3	5	9	12	17	22	25
3DES	2	2	6	8	12	20	27	30

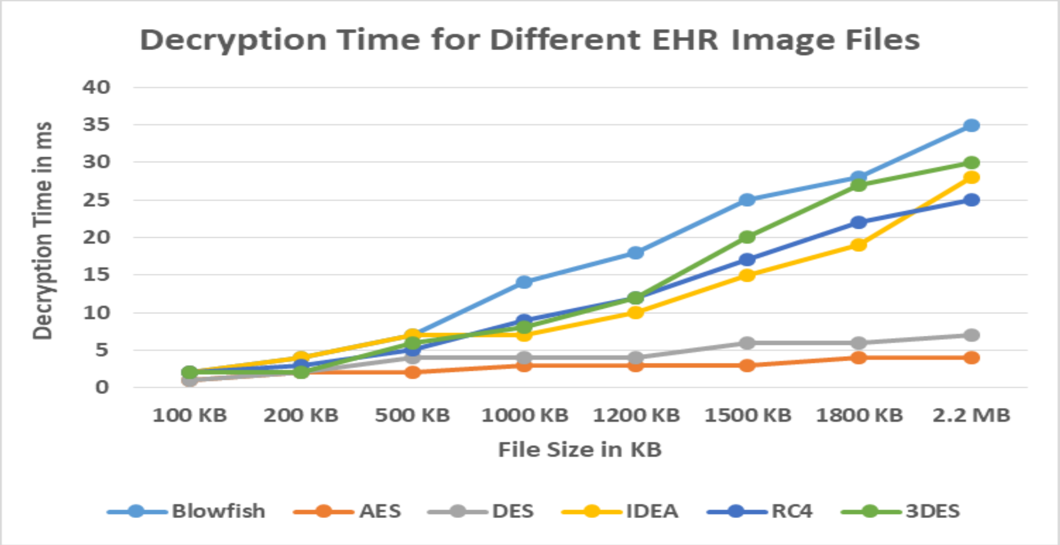

Figure 4: Decryption times for different image files

CONCLUSION

In our study, it is found that, AES is the best performed algorithm than other algorithms. Blowfish has average rate of performance. Blowfish is the second best performed algorithm for EHR contents text and image.

The symmetric key algorithms take less time than asymmetric key. We can suggest that, for electronic health record content transmission symmetric key algorithms should be use.