Journal of Theoretical and Applied Information Technology
30th June 2018. Vol.96. No 12
© 2005 – ongoing JATIT & LLS

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

TEXT CRYPTOGRAPHY USING MULTIPLE ENCRYPTION ALGORITHMS BASED ON CIRCULAR QUEUE VIA CLOUD COMPUTING ENVIRONMENT

[1]KHALID KADHIM JABBAR, [2]HUSSIN ABD HILAL, [3]RANA SAAD MOHAMMED

[1] University of Mustansiriya, College of Education, Department of Computer Science, Iraq
[2]University of Mustansiriya, Electronica Computer Center Department, Iraq
[3] University of Mustansiriya, College of Education, Department of Computer Science, Iraq
E-mail: [1] khalid_jabbar@yahoo.com, [2] husseinabed342@gmail.com, [3] Ranasaad2014@gmail.com

ABSTRACT

The tremendous development of communication technology, it has become necessary to use cloud computing systems that help us to store the data within a virtual structure, with the increasing volume of important data, the need to secure this data has become necessary through the use of diverse and complex techniques and methods to ensure integrity, confidentiality, and security. This paper presented a method to encrypt a message with different sizes in cloud computing environment by using several encryption algorithms such as: Advanced Encryption Standard AES, Advanced Encryption Standard RSA, and Advanced Encryption Standard Proposal AESP to make the method more secure and effective. which controlled by circular queue that is responsible for scheduling the implementation of the algorithm that defined by a secret code generated by Control Key, this a secret code is changed each time and with each message to be decoded later by using the same secret code to infer the algorithm that used in the encryption, in addition to the possibility of generating multiple random keys that are vary according to the encryption algorithm used. The experiment results shows that the proposed method has ability to encrypt and decrypt a text message with different sizes and short time by utilizing the properties of several algorithms that are scheduled on circular queue inside the cloud computing system, the proposed method consume time is less than other methods when it used alone, while the important criteria such as integrity, complexity, usability, and security are take into consideration to make the method more effective and efficient.

Keywords: *Integrity, confidentiality, RSA, AES, AESP.*

1. INTRODUCTION

The rapid development in the field of communications technology and multimedia has become so great that most consumers of this technology prefer to use the Internet as a primary medium to transfer their data from one party to another. And with the diversity of modes of transport multiple which became possible for all such as: e-mails, chats, social media, etc. Where data is transferred in a simple, fast and accurate using these means; moreover, these services are not a major problem in the transmission of data over the Internet but represent a security threat to the confidentiality of this information through the theft of personal or confidential information in many ways. It is therefore very important to consider data security, confidentiality to prevent data from unauthorized users or hackers from Stolen it, figure 1 illustrate the data security fields. One of the important filed called the cryptographic that can be grouped into four fields. Symmetric encryption that used to hide the contents of blocks or streams of data with any size, such as: including messages, files, encryption keys, and passwords. While asymmetric encryption: used to hide small blocks of data, which are used in digital signatures, such as: encryption keys and hash function values.

Data integrity that used to protect a blocks of data, such as: secret messages, from alteration. And the authentication protocols: These are methods based on the use of cryptographic algorithms designed to authenticate the identity of structure.

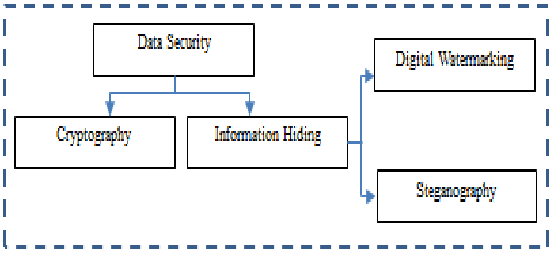


Figure 1: Data Security

Cloud computing system provides the requirement that needed to access from a shared pool of computing resources such as; hardware and software for effective manage performance, and increasing the control and security of data for data owner by outsourcing to serve a user data inside cloud environment, to maintain the control of data within networks and offers more advantages for data security. Protecting the important data in the cloud, authentication, access control, encryption, integrity checking and data masking are some of the data protection techniques. Cryptography is the one of an efficient methods for data security in cloud computing. System, it includes the design and implementation of an effective encryption and decryption algorithms. The research motivation of the proposed method is to demonstrate the possibility of encrypting the confidential text message within the cloud environment using a set of known encryption methods for its ability to encrypt and preserve the confidentiality of secret message, as well as to utilize the characteristics of the circular queue structure that processes the encryption process of the confidential message, each time encrypt the secret message with an method to add an additional level of complexity, confidentiality and security to encrypt the text message while keeping the time factor to be short during the implementation process. The primary goal of our proposed method is to develop a method that has ability to encrypts a secret message according to several standard algorithms that use in this filed inside the cloud computing system, this algorithms are scheduled in circular queue that controlled its input and output, several stages and processes are used to complete our goal. The following sections are organized as follows: Section 3 introduced RSA, AES, AESP, and LFSR briefly, While section 4 talk about the related attempts, the proposed method illustrated in section5, the results that extracted shows in section 6, while section 7 illustrate the conclusion.

2. RSA, AES, AESP, and LFSR

In [1] the mathematics of RSA algorithm is relatively simple to implements. The public and private key created by define a two bigger prime numbers named (P, Q), then, N calculated as: $N=P*Q$, while $\phi= (P-1)(Q-1)$, since the selected random integer e, must be in the range of $1<e<\phi$, where $\gcd(e, \phi) =1$. Furthermore, d calculated by using the extended Euclid's where $ed =1 \bmod \phi$. Since, the Public key = (n, e) and private key = (n, d). The following steps illustrate the encryption stage:

1. Obtain the public key (e, n).
2. Represent the plaintext to as an integer. Encryption using the equation $c = m^e \bmod n$. While the Decryption stage illustrated in the following simple steps:

- Used the private key (d, n).
- Decryption using the equation $m = c^d \bmod n$.

Another algorithm that adopted in [2], talk about the Advanced Encryption Standard (AES) that adopted by the National Institute of Standards and Technology of the US Government as a formal encryption method. A several rounds for encryption process with encryption key are used to in the encryption algorithm that called a block cipher and the work as a single unit of data at a time. In standard case, the block cipher may be 128 bits, or 16 bytes, while each round depended on the length of the key. The single key that used in encryption process with size of: 128 bits (16 bytes), 192 bits (24 bytes), or 256 bits (32 bytes). Furthermore, AES uses the same key in encryption and the decryption processes. While [3] proposed algorithm include of five layers in each round (number of rounds is 14 round), and it's based on modifying the structure of (AES) algorithm, After 14 round are completed, then a 256 bit as input will be 512 bits, while each round will get 512 bits will be split in to the two parts (odd, even) bits by using split function. Furthermore, the odd bits will be encrypted by using Al-Gamal Public Algorithm, the results saved in buffer; on the other hand, the even bits will go to the next 14 round. The buffer that saved the last results for the odd bits still stored the same file of the encryption, mean all result save in one not two file while that file send to destination after the 14 round are completed. A linear-feedback shift register (LFSR) is a shift register that illustrated in [4]; the input bit is a linear function from its previous case. The exclusive-or (XOR) represent the most commonly function that used in linear function. This shift register generate a series of bits that become as random bits with a very length cycle. The most common using for the LFSRs is generating bogus random numbers, bogus noise sequences, and rapid digital counters.

3. THE RELATED ATTEMPTS

Keep data in the cloud environment secure need to use some of the data protection techniques such as: authentication, integrity, access control, encryption, integrity checking and data masking. Encryption process is the one of the most commonly way that used to protect data in cloud computing system. The main techniques that used to manage the data protection in the clued are: directory level, full disk level, application level and file level. Some of these methods that used in the field of protection data inside cloud computing system are: the method that presented in [5] based on RSA, the cover organized into several blocks of circular queues. The embedding process dynamically is employed to assign secret cypher blocks to circular queues, while a receiver will use private key in RSA to determine the right plain text. While [6] proposed effective encryption method to encrypt important data before sending to the cloud server, based on the block level data encryption by using 256 bit symmetric key with rotation, the reconstruct process depending on the same secret key to reconstruct the original message, the exclusiveness's protection performed over all the warehouse of text files with variable size. The security and performance analysis shows that the proposed method is highly efficient than existing methods performance. Other attempts that done by [7], presented a business way in cloud computing for important data security using the standard data encryption \decryption algorithms. The responsibility of cloud service provider is for data storage and data encryption/ decryption processes. The essential disadvantage is there is no control in this method.

4. THE PROPOSED METHOD

Cloud computing system is serving several fields such as: application, connectivity, and storage. Each of them serves a multipurpose that produced an essential application that helps the businesses around the world. The proposed method depends on a set of techniques and methods that integrated into one application with several stages, in order to ensure the efficiency, integrity, security and quality of the results in the terms of speed, complexity in the processes of encrypting and decrypting of the confidential text message within the cloud environment. The proposed method consists of the following stages:

1. Several encryption/ decryption algorithm such as: RSA, AES, and AESP stages, that illustrated in section 2.
2. Circular queue process.
3. Polynomial (poly) technique processes.
4. Control key process.
5. Key string stage, this stage include the following processes:

a. Key string generator.
b. Convertor function.

6. Encryption stage.
7. Decryption stage.

The first step in the proposed method begin with the login to the cloud, the figure 1 illustrates this process:

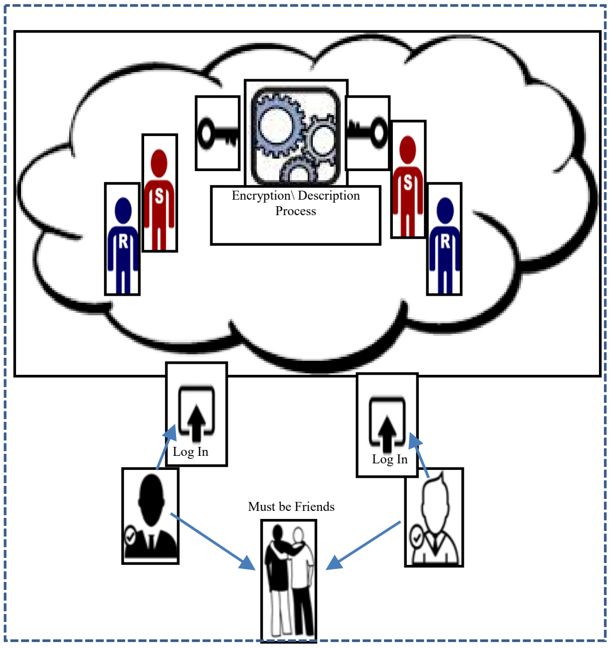


Figure 2: The Process of Login with cloud System

4.1 Circular Queue

Linear data structures have some weaknesses, especially in the optimal utilization of the memory space. Since there is a need to use another type of data structures that can exploit the available space without wasting in the remaining space. So the used of circular queue solve this problem, circular queue is one of the data structures that used in the process of organizing storage, retrieval of data or improving the performance of the systems by taking advantage of the possibility of this data structure to exploit all the available space without wasting in the memory area. In the proposed method, the circular queue is a very important part because it is responsible for determining which of the algorithms that used will come into effect. The size of a circular queue starts from position 0 to N-1, and the declaration of circular queue aimed to allocate some of the sites in the memory as: S_v, algorithm 1 illustrate this declaration:

```
Algorithm 1: Circular Queue.
Input: Max number of Process as: $M_p$.
Output: The series of available locations as: $S_v$.
        Begin
            Define Max number ($M_p$);
            Int c.queue [$M_p$];
            Int front= -1, rear= -1;
          END;
```

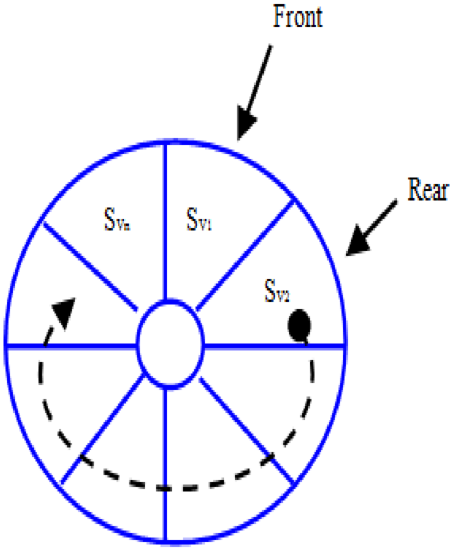


Figure 3: Circular Queue

The encryption algorithms will enter to the queue successively, and according to their sequence, On the other hand, the circular queue that used in the proposed method work with the process of control key to give each algorithm is ready to implement a secret number to be used in the decryption stage latter.

4.2 Polynomial Process

The key string is generated in this process, which is a random key that exposed to the five tests for detecting the randomness. Furthermore, our proposed method added some development through the use of six exponential equations starting from the third to the sixth degree for the left and right sides. Note that the equations used differ from each other and also relied on a set of tests in the test of these equations in order to get the largest number of keys.

The following algorithm illustrates a poly process:

```
Algorithm 2: Polynomial Process.
Input: Sex equations.
Output: key string as K_s.
   Begin From the right side.
      Read the string of bits from 3, 4, and 6
      polynomial;
      Apply LFSR to generate the key of string
      form according to the length of polynomials;
   END.
```

4.3 Control Key

In this part of our proposed method, a secret code is given to the algorithm that enters into force in conjunction with the circular queue according to the algorithm exit time of the waiting process in the circular queue, all algorithms that used in the proposed method will be represented as a processes (A_1, ...A_n), and each one has a specific time for the process of entering to the circular queue that represented as: A_T, while each process remaining in the waiting period until the time of implementation depending on the A_T. The secret code is given to each process based on the time of entry into the circular queue, this secret code is selected by the control key, and this secret code has no relationship with the period of its stay in the circular queue.

The secret codes given to each algorithm are not repeated and are inferred to it only by the control key process. Accordingly, the appropriate code and decoding keys are selected, taking into consideration the type of algorithm based on a number of factors and criteria, including:

i. RSA: The initial key must be a component of 3 digits or more.

ii. AES: One key needs for encryption and decryption stage. The length of the key must be between the range of 64, 128, 256 based on the type of algorithm.

iii. AESP: Three keys are used for encryption and decryption stage:

  a. One key dedicated to the 256 bit for AES algorithm.

  b. Two keys assigned to the RSA algorithm based on the RSA criteria for selecting custom keys.

4.4 Key String Stage

a. Key string generator.

In this process, the encryption\decryption key is generated by the key string generator depending on the algorithm code that obtained from the control key process. Furthermore, the poly process generated a string of 4000,000 bits that used to produce a key string. The following figure shows the process of key string

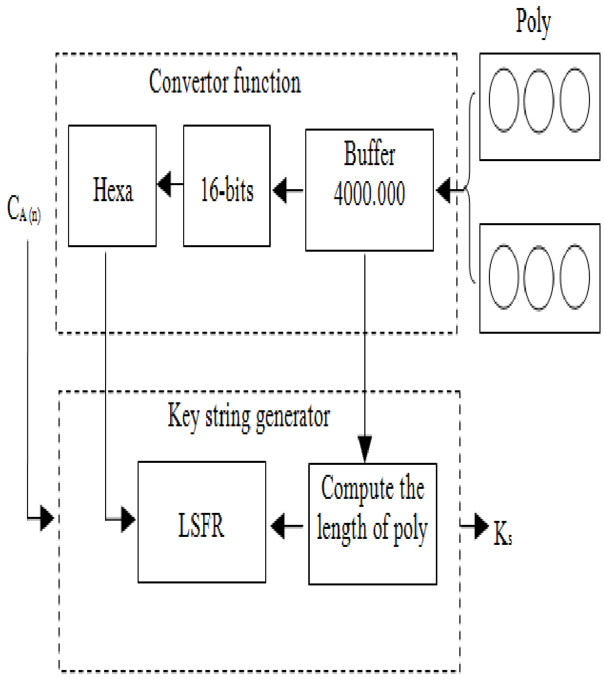


Figure 4: Key String Stage

From polynomial function that used 6 polynomials (3 polies in the left side, 3 in the right side) these 6 polies are used to generate a huge number of bits. The huge bits are store in buffer (0…..n-1), while it used to in the other generator (key string). The same bits that stored in the buffer are used to compute the length of poly L_p, since, L_p, $C_{A\ (n)}$, and LSFR are used to generate K_s.

b. Convertor function.

In this process, the huge bits that produced by polynomials functions, the convertor process cut only the 16-bits from the left hand side, then all that converted into the hexa units, then go to the LSFR. The same bits needs by the receiver side with decryption stage.

5. ENCRYPTION STAGE

This phase of the proposed method involves encrypted the message in the side of a sender O_t by one of the three encryption algorithms that illustrates in the existing paper. The chosen algorithm $C_{A(n)}$ that used in the encryption process based on the randomly, and its secret selection that changes for each time and with each O_t in a highly confidential random manner. The encryption stage requires the K_S that is generated in the key string stage, in addition to the original message Ot. So, the encryption process is now ready to be applied to the O_t being sent to produce $O_{t'}$ after encryption stage is complete. The following figure shows the encryption stage, while algorithm 3 illustrates the main steps for this stage:

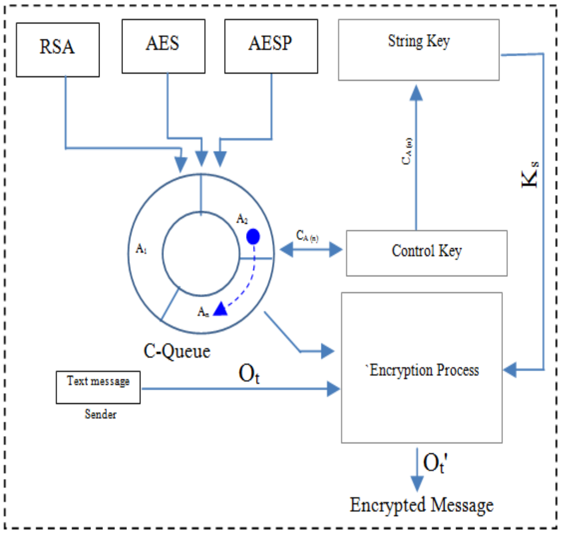


Figure 5: Encryption Stage

```
Algorithm 3: Encryption Stage.
Input: $O_t$, $K_s$.
Output: $O_{t'}$.
 Begin
   Read $O_t$;
     According to the circular queue and control key
     the $C_{A(n)}$ produced, and the encryption algorithm
     (RSA, AES, or AESP) will be chosen; Apply
     $C_{A(n)}$ according to $K_s$ over the $O_t$ to produce $O_{t'}$;
     END.
```

4.5 Description Stage

In the following figure, the decryption stage includes two basic processes that are: convertor function and control key in addition to the basic stage of encryption; while algorithm 4 illustrates this stage:

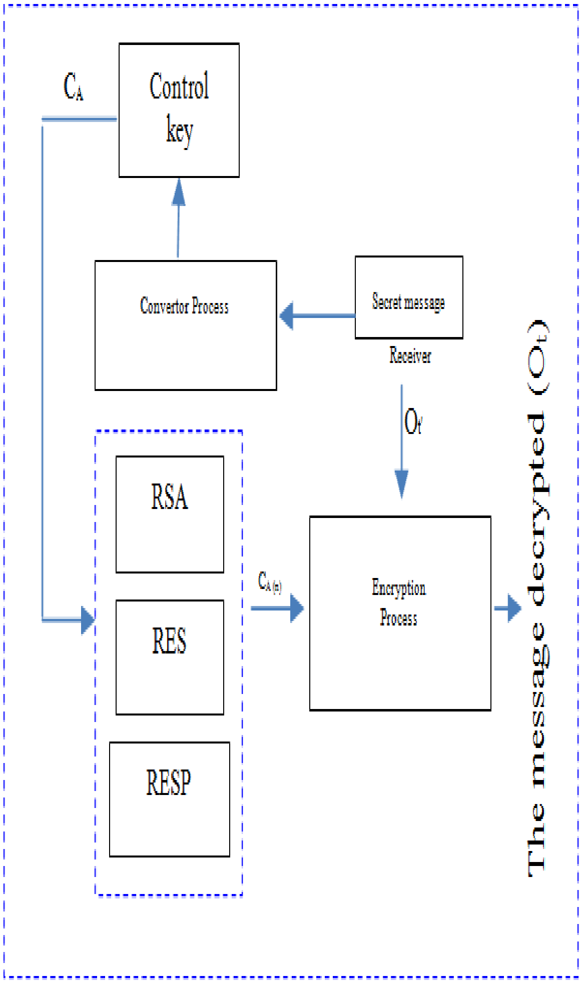


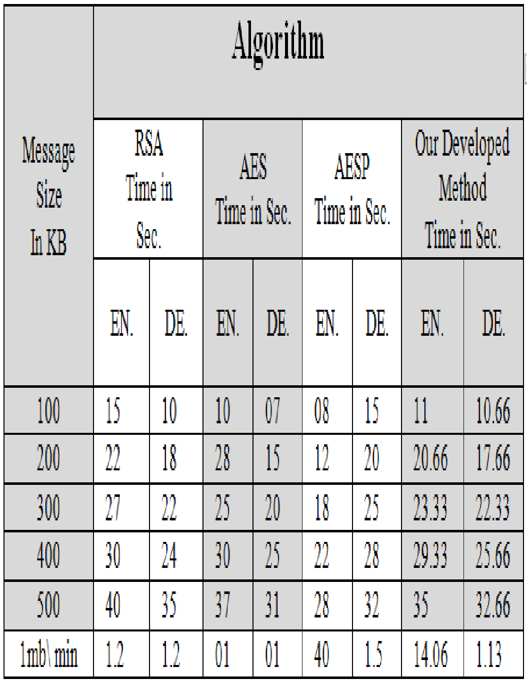
Figure 6: Decryption Stage

```
Algorithm 4: Decryption Stage.
Input: $O_{t'}$,
 Output: $O_t$.
   Begin
      Read $O_{t'}$;
       Choose $C_A$ according to the convertor function and control key to produce $C_{A(n)}$;
       Apply the appropriate algorithm over the received $O_{t'}$ according to the $C_{A(n)}$ to produce $O_t$;
   END.
```

6. RESULTS

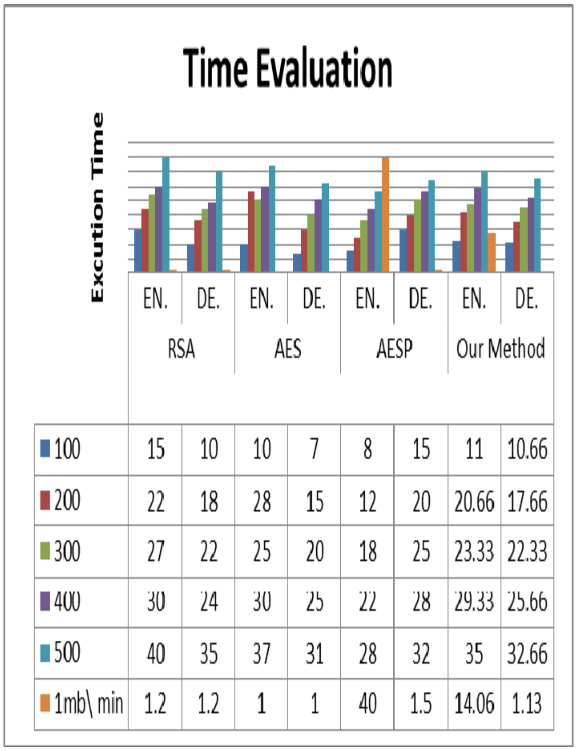
In the field of data encryption and decryption the main factors that used to measure the security and performance for the proposed method are: complicity, execution time, security, confidentiality, Integrity and usability, and Key length. Our paper describes a method that includes encryption of data by using the standards encryption algorithms. By doing so, the extracted results can be adequate secured and thus can help in further enhancement of the cloud computing security. Table 1 illustrates the execution time with different messages size of our proposed method that compared with the other method.

Table 1: Time in Second and Minute



Message Size In KB	Algorithm							
	RSA Time in Sec.		AES Time in Sec.		AESP Time in Sec.		Our Developed Method Time in Sec.	
	EN.	DE.	EN.	DE.	EN.	DE.	EN.	DE.
100	15	10	10	07	08	15	11	10.66
200	22	18	28	15	12	20	20.66	17.66
300	27	22	25	20	18	25	23.33	22.33
400	30	24	30	25	22	28	29.33	25.66
500	40	35	37	31	28	32	35	32.66
1mb\ min	1.2	1.2	01	01	40	1.5	14.06	1.13

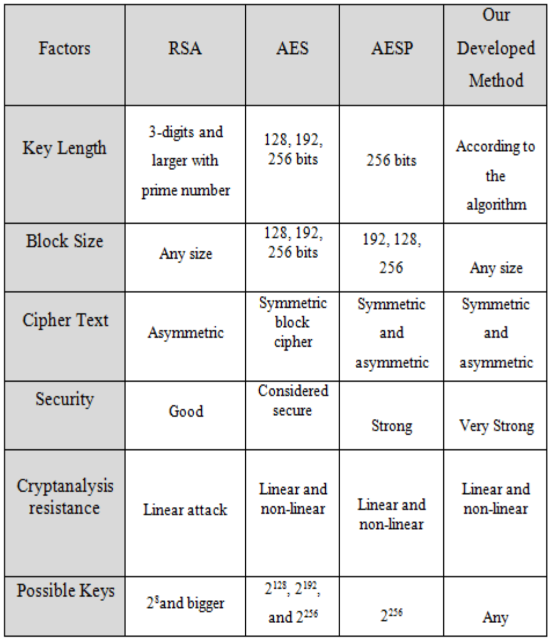
The time factor is an important factor that used in evaluating the encryption\ decryption method. In the table above, the variance in the time of encoding and decoding process was depending on the type of algorithm used, taking in the account that the time is increasing with the increase in message size used. While, in our proposed method; this discrepancy was controlled, and reached a stage of balance in the time taken in the coding and decoding process, although the algorithm that used each time was different because of the nature for the circular queue that regulated the process, time difference was less compared with methods if each method used as alone. The using of circular queue for controlling the executing time for each algorithm depending on the control key and arrival time to the circular queue that led to the creation of a balance at the time of implementation and reduction of variance in this factor as shown in the table above. The next figure shows the evaluation time for the proposed method. While the other factors that used to evaluate the performance of our proposed method with other methods shows in table 2:



	EN.	DE.	EN.	DE.	EN.	DE.	EN.	DE.
	RSA		AES		AESP		Our Method	
■100	15	10	10	7	8	15	11	10.66
■200	22	18	28	15	12	20	20.66	17.66
■300	27	22	25	20	18	25	23.33	22.33
■400	30	24	30	25	22	28	29.33	25.66
■500	40	35	37	31	28	32	35	32.66
■1mb\ min	1.2	1.2	1	1	40	1.5	14.06	1.13

Figure 7: Evaluation the Execution Time

Table 2: Compare the Performance According to Combine Several Algorithms



Factors	RSA	AES	AESP	Our Developed Method
Key Length	3-digits and larger with prime number	128, 192, 256 bits	256 bits	According to the algorithm
Block Size	Any size	128, 192, 256 bits	192, 128, 256	Any size
Cipher Text	Asymmetric	Symmetric block cipher	Symmetric and asymmetric	Symmetric and asymmetric
Security	Good	Considered secure	Strong	Very Strong
Cryptanalysis resistance	Linear attack	Linear and non-linear	Linear and non-linear	Linear and non-linear
Possible Keys	$2^8$and bigger	2^{128}, 2^{192}, and 2^{256}	2^{256}	Any

The use of the circular queue in the proposed method was come for take advantage of the method of organization used in this structure, which depends on the exploitation of the entire available storage space in order to increase the quality of performance of this data structure in order to overcome the problems that are can encounter if use the simple queue. Each algorithm that used in the proposed method has been treated as a stand-alone process and not overlapping with other processes that deal with the same secret message later using a set of assistive techniques that will be discussed in detail later. The method that used for each algorithm to be implemented on the secrete message make it impossible to guess the type of method used in encryption and decryption is difficult, which increased the degree of complexity and thus the security of a secrete message and the proposed method has become secure. As the proposed method ensures dealing with different algorithms that work in the field of encryption and decryption regardless of its type or complexity of it. our proposed method provides an interactive environment integrated and non-overlapping can be activated any algorithm and extract the results within a short period of time without there is any loss in time or quality, the complexity factor will be increased as the number of algorithms increases, in addition to the emphasis on the principle of ease of use and balance in the results extracted without there being a large difference in it. The results that presented in the table 2 summarized prepared according to a comparison between our proposed method and a range of methods that dealt with the same filed.

The extracted results are good, especially in the field of balance that was achieved in our proposed method in all factors that showed in the different tables in the existing paper. For the length of the key, it noticed that there was a difference key length from one method to another according to the structure and complexity of the method, and since the proposed method presented a model that combines different the algorithms that were pre-presented in a single integration environment and thus the length of key for the proposed method varies depending on how you will be under implementation depending on the choice of circular queue. On the other hand, the proposed method works according to any size and without any restrictions on in the block size. While in the cipher text, it variable according to the algorithm that worked at a time in where it can be symmetric or asymmetric and this factor provides high flexibility to work.

Security factor is one of the most important factors that used in evaluating which method works within this area, and our proposed method focused on the security and confidentiality side and the associated time factor in order to achieve the highest level of efficiency and quality in the process of encrypting and decrypting to the secret message. Our proposed method used a set of algorithms which is adopted in this field and placed them within a single integrated environment that controlled through the use of the circular queue, which regulates the process of entry of the specified algorithm into operation and work separately and without any overlap or any error in performance, which provided the principle of integration on the side of construction, that make it difficulty of guess the style used in the encryption, which increases the degree of complexity and the security aspect of the proposed method. When talk about possible key, it is not specific. It can change each time and according to the method in the performing process.

The proposed method provides high flexibility and non-specificity factor by integrating more than one algorithm into one interactive and integrated environment. Other properties that can be noticed illustrated in the following table:

Table3: Performance Evaluation according to Other

Characteristic	RSA	AES	AESP	Our Developed Method
Time requirement	More	Less	More	balanced
Confidentiality	More	More	More	More
Integrity and usability	More and long text	More and long text, and short text	More and long text, and short text	More and long text, and short text
Key length	More	Less	More	Flexible

Our proposed method is characterized by increasing the complexity associated with the process of encryption, which makes the process of guessing or detecting the original message is difficult, through the using of different encryption algorithms every time the secret message is encrypted and therefore the increase in the security aspect of the proposed method is significant. The time that will take during encryption and decryption process is clear when it compared with other methods, which vary in time of encryption and decryption. The limited application of the proposed method in a specific area of multimedia can be considered a weakness of the proposed method. The proposed method was built on the basis of a set of known cryptographic algorithms, some which developed from the integration of a set of methods in one way. The new in the proposed method is the use of the circular queue as the main pivot that organizes the encryption and decryption process, the mechanism illustrated in the section of the proposed method.

7. CONCLUSION

The experimental side of our proposed method, which was supported by the results, proved that the proposed method has the ability to encrypt and decrypt the confidential text message with high flexibility and confidentiality by using different methods of encryption based on the mechanism that provided by the circular queue with the provision of time factor. After comparing with the other methods, it found that the proposed method achieved balance and reduce the time factor during the process of encryption and decryption, and this is a proven in the results side. On the other hand, Cloud computing is one of the most important communication systems in use today, and the most applications inside the cloud computing system are interested in maintaining the confidentiality of information that is traded within the cloud environment through the use of traditional encryption methods in different ways to increase and to enhanced the security aspect for the important information. One of the most important measures that used in measuring the quality of the method used is the time factor, which plays a major role in reducing the time of encryption and decryption stages. The less time, the better proposed method, with emphasis on the factor of confidentiality, integrity, and complexity. In other words, each method uses a specific algorithm for encryption and decryption stages and each algorithm has specific time for implementation is different with the other algorithm. On the other hand, the size of the document varies from one to another; this factor is added to the set of determinants affecting the quality of the proposed method. In this paper, a simple method was introduced that makes encryption and decryption stages different from time to time. In other words, each document is handled in a different way from the other documents through the use of the several encryption algorithms based on a circular queue which regulates the process of entering each algorithm to the queue as a process that enters to the circular queue according to its arrival time to the queue without affecting to the nature of algorithm or execution time factor.

This operation make a balance in the time that spent by each algorithm is almost equal with all algorithms that used in our proposed method. The performance of the proposed method was evaluated through a set of tests. After collecting the data, we concluded that the proposed method has the ability to secure a data transmitted between the sender and receiver within the cloud environment, while ensuring the speed, accuracy, complexity, and integrity during the encryption\ decryption process.

REFERENCES

[1] Nentawe Y.,"Data Encryption and Decryption Using RSA Algorithm in a Network Environment", *IJCSNS International Journal of Computer Science and Network Security*, July 2013, VOL.13 No.7.

[2] Roshni P., Aamna U.,"Encryption and Decryption of Text Using AES Algorithm"; *International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal*, May 2014Volume 4, Issue 5.

[3] Hussein A.," Proposed a Private Cloud Cryptography Model", *MSc. University of Technology, Computer Science Department*, Baghdad, 2015.

[4] Geremia P. "Cyclic Redundancy Check Computation", An Implementation Using the TMS320C54x" , *Texas Instruments*, 2016.

[5] Mamta J., Saroj K., Sunil K.,"Adaptive Circular Queue Image Steganography with RSA Cryptosystem", *Elsevier, Perspectives in Science 8*, 417—420, 2016.

[6] Prakash *G*., Manish P., Inder *S*.," Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System", *International Journal Of Engineering And Computer Science* ISSN:2319-7242 Volume 3 Issue 4, April, 2014, Page No. 5215-5223.

[7] Jing J., Taoyuan, Taiwan Y., Chien H., "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service", *International Conference on Information Science and Applications (ICISA)*, pages 1-7, 2011.