International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Research Paper Volume-5, Issue-4 ,2018 Regular Edition E-ISSN: 2349-7084

Performance Analysis of Various Encryption and Multilevel Encryption Techniques for Cloud Computing Security

Prof. (Ms.) Kimaya Ambekar[1], Prof. (Dr.) R. Kamatchi [2]

[1]*Asst. Professor, Somaiya Institute of Management Studies & Research*

[2] *Professor, Amity University*

Available online at: http://www.ijcert.org

Received: 18/April /2018, Revised: 19/April /2018, Accepted: 24/April /2018, Published: 27/April/2018

Introduction:

Cloud computing is seen as unlimited amounts of Information technology resources which can be used as services through the Internet and from any device as well as from any corner of the Globe. According to NIST definition, Cloud Computing can be divided into various types depending on its service provision and deployment strategies; Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS) depending on service provisions and Public, private, community and hybrid depending on deployment strategies. According to researchers, 85% of organizations have used a multi-cloud approach, which was 82% in the year 2016 [1]. Also, use of public cloud has risen by 4% from 67 to 71% in this year. Slowly and steadily, organizations across the world and in every sector are using the cloud in some way or other. Still, the number has not improved as expected by the cloud market players. The major reason behind the resistance is Security and privacy of the data in transit and stored at Cloud Service Provider's (CSP's) end. Though the SLA (Service Level Agreement) defines all major attributes related to security, availability, and reliability of the data

Organizations are hesitant to use Cloud comprehensively. Data is the most important asset for any organization and preservation of that become essential. The CIA security triad i.e. Confidentiality, Integrity, and availability is a model considered to monitor rules for information security. The major issue is considered as confidentiality. It deals with unauthorized

Or unauthenticated access to the data. This can be solved by cryptography. Hashing algorithms can solve integrity. This paper uses a cloud security model and tries to evaluate the effect of different encryption algorithms in the model. The inclusive outcome of different algorithms and multi-level encryption algorithms are analyzed based on different performance evaluation parameters.

The scope of the Study:

Security is the most concerned part of cloud computing. That is why encryption becomes very important in the cloud environment. Many researchers have concentrated on the encryption algorithms used in the cloud to understand the performance.

The authors in [2] described a model which used VPN and a combination of various techniques like SSO, Multilevel authentication etc. Authors have proved VPN provides security and it gives improved response time than the normal firewall. The paper also suggests servers' placement in public and private cloud.

 https://doi.org/10.22362/ijcert/2018/v5/i4/v5i405

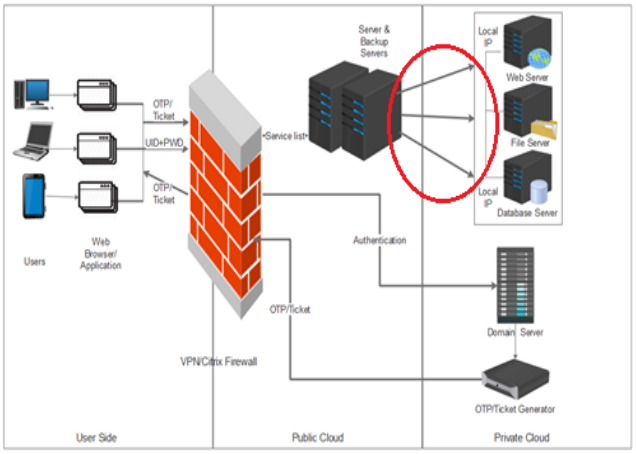

Fig 1: Cloud Security Model [2]

There will be a communication between them to serve the users. The data flowing through public and private cloud needs to be secured. We can introduce various encryption techniques in that area to make the model more secure. In addition, depending on the criticality of the application or data, we can also use multi-level encryption. This paper evaluates various cryptographic algorithms on some important parameters like encryption and decryption time, memory used, throughput etc. This paper also checks the performance of various multilevel algorithms.

Background Study:

Cryptography is a practice and study of secure communication in which message is encrypted in the ciphertext. The major purpose is to hide the correct data from unauthorized users. The message will be encrypted at sender's end and can be decrypted at receiver's using same or different keys depending on the algorithm used in the process

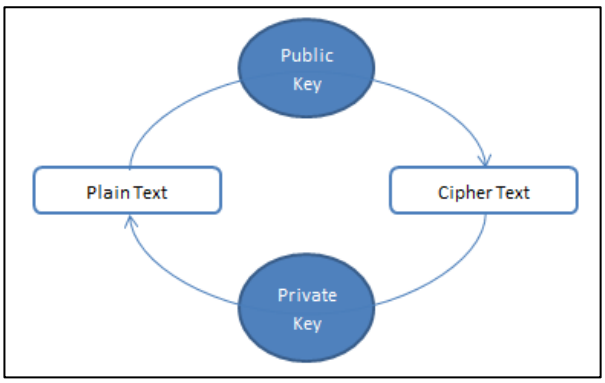

Fig 2: Encryption/Decryption Process [3]

There are 2 major types of cryptography. They are Symmetric and asymmetric key cryptography.

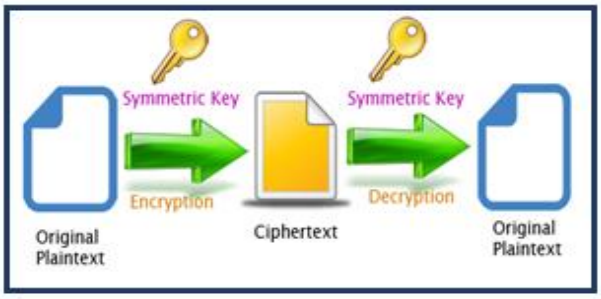

Fig 3.a: Symmetric key cryptography

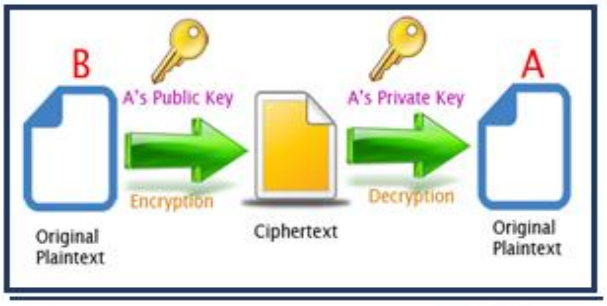

Fig 3.b asymmetric key cryptography [4&5]

As shown in figures, symmetric key cryptography access one single key to encrypt at sender's side and for decryption at receiver's side [6]. And inverse to that in asymmetric key cryptography, one key which is also called as a public key, is shared with everyone Sender uses the receiver's public key to encrypt the message and receiver use its private key to decrypt the message. There are various algorithms written for both the type of techniques which all have their own positives and negatives. The following figure can illustrate the different types of algorithms.

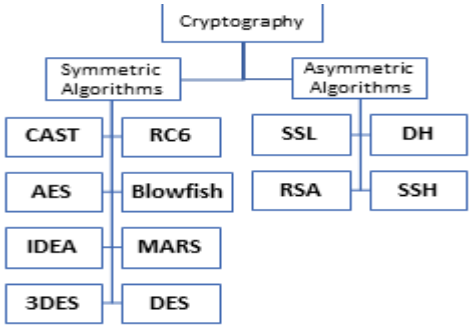

Fig 4: Different Algorithms for symmetric and asymmetric key algorithms

Both the approaches have their pros and cons. Symmetric key algorithms come with the key transportation problems. The secret key should be transported through the data to the receiver to decrypt the data; on the other hand, asymmetric key avoids this problem since it uses different keys for encryption and

decryption. Because of this reason, asymmetric algorithms provide better security than symmetric. But symmetric algorithms are proved faster than asymmetric algorithms. Since cloud computing involves a huge amount of data, speed makes an important parameter for the adoption of algorithms in cloud computing. [7]

Classification of Algorithms in Detail:

1. Symmetric Key Algorithms:

- **The DES Algorithm (Digital Encryption Standard):**

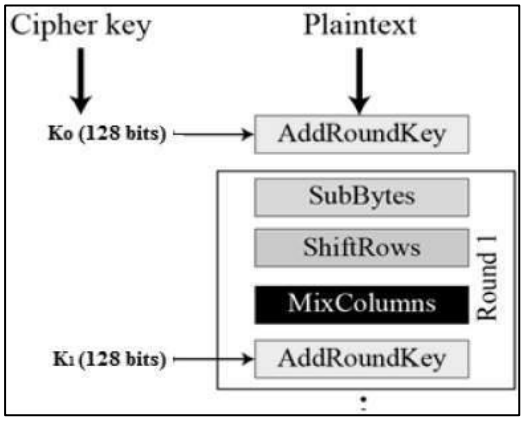

Fig 5: DES Algorithm [8]

It is Feistel Cipher implementation with 16 rounds. Both block size and key length are 64 bit but 8 bits in key length are used as check bit so the actual key length becomes 56 bits. Due to the smaller size of the key, the encryption is vulnerable to code-breaking efforts like Brute force attacks. But as the rounds of substitution and transposition increases, it may show good effects.[9&10]

- **The 3DES Algorithm:**

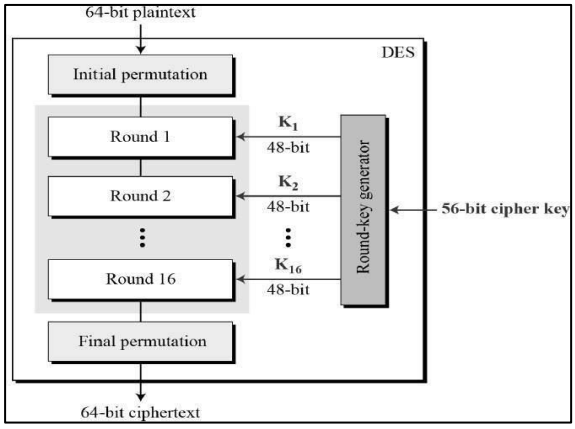

Fig 6: 3DES Algorithm

It is an enhanced version of DES. It also shows block size of 64 bit and a key size of 56 i.e. 64-8. The only difference is, 3 keys are used instead of one, and therefore total key-length becomes 168 bit. It eradicates the short key problem of DES. This algorithm comes in 2 versions 2DES & 3DES. It obviously gives better security at the cost of time consumed for encryption and decryption. [11]

- **The Blowfish Algorithm:**

Auxiliary to DES or IDEA algorithm, blowfish can be seen. It shows 64-bit block size and variable length of key ranging from 32 to 448 bits. Similar to CAST algorithm, it also uses fixed s-box structure. Generally works with 16 rounds of Feistel Cipher. It is one of the fastest block cipher algorithm. Excluding the time when you need to change the key, it needs a processing correspondent to 4KB of text encryptions. It is not patented and easily available for the users. It generates a large key so it provides a greater security.

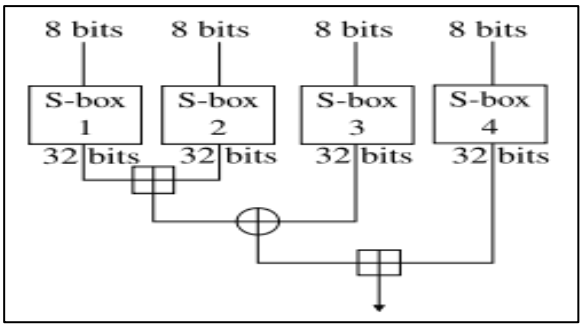

Fig 7: Blowfish Algorithm

- **The AES Algorithm (Advanced Encryption Standard):**

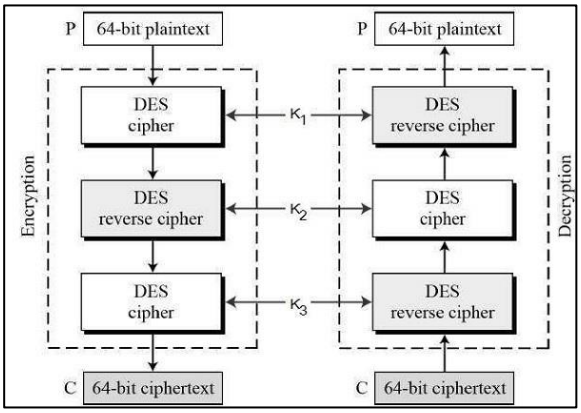

Fig 8: AES Algorithm [12]

This algorithm includes 3 major blocks of a cipher, they AES-128, 192, 256. Each cipher is responsible for encrypting as well as decrypting the blocks of 128bits. It uses 3 different steps to provide the

better security from its ancestor algorithms and they are transposition, substitution, transposition- substitution respectively. [13], [14]

2. Asymmetric Key Algorithm:

- **Diffie-Hellman (DH) Algorithm:**

This is a method by which one can securely exchange the secret mostly a secret key over an insecure communication channel. Before two parties want to start sharing information, the key needs to be shared by which two parties can encrypt the data. DH protocol is used for sharing this key among the parties.

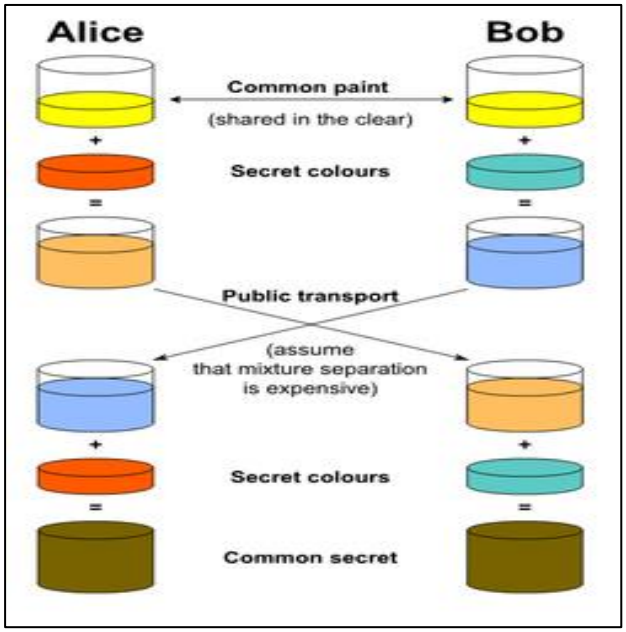

Fig 9: Diffie-Hellman (DH) Algorithm [15]

RSA Algorithm:

Rivest–Shamir–Adleman is most common for secure data communication. Here, the encryption key is publically shared and for decryption, the secret key is used. The public key which is shared with everyone is based on 2 large prime numbers. This key is used to encrypt the message. Since it uses prime numbers, it is relatively difficult to crack the algorithm. Still, it is found that this algorithm is relatively slow [16]

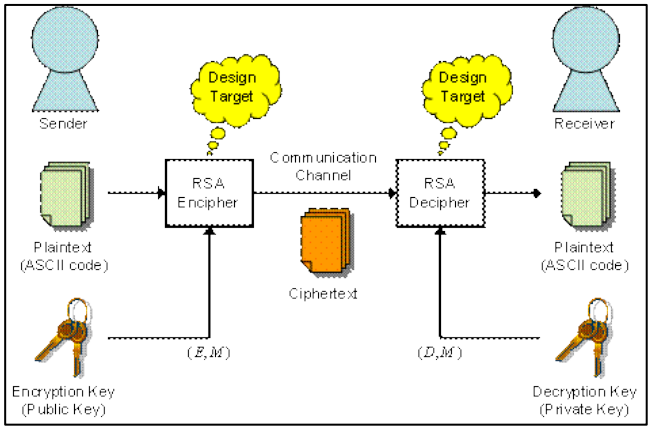

Fig 10: RSA Algorithm [17]

Algorithmic Description:

	AES	DES	3DES	Blowfish	RSA
Name	**Advanced Encryption Standard**	**Data Encryption Standard**	**Triple DES**	**Blowfish**	**Rivest–Shamir–Adleman**
Key Size	128, 192, 256	56	168	32-448	1,024 to 4,096 bit typical
Block Size	128	64	64	64	128
Rounds	10,12,14	16	48	16	1
Algorithm Structure	Substitution - Permutation	Feistel	Feistel	Feistel	Factorization

Performance Evaluation Parameters:

There are various criteria to evaluate any algorithm's performance. There are few which are taken into consideration for this paper. They are as follows

- **Encryption Time:** The encryption time considered the time that an encryption algorithm takes to produces a ciphertext from a plain text.
- **Decryption Time:** The decryption time considered the time that a decryption algorithm takes to produces a plain text from a ciphertext.
- **Memory Used:** Different encryption techniques require different memory size for implementation. This can be different for different types of algorithms. Memory used is calculated using number & types of operations required for the algorithm and also the key size used for encryption/ decryption process.
- **Throughput:** How much information is processed at a time

$$\textbf{Throughput} = \frac{\textbf{Total plaintext}}{\textbf{Encryption Time}}$$

Implementation:

In the research paper, we have identified and implemented most suitable and popular cryptographic algorithms for analysis purpose. We have used Visual Studio 2017 for implementation purpose. The application takes any file or textual data as an Input and provides the detail evaluation of the various parameters. The implemented application looks as follows

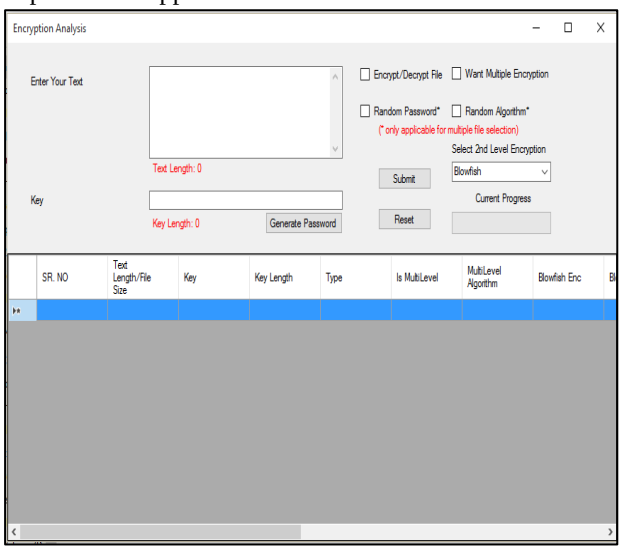

Fig 11.a Application showing basic functionalities.

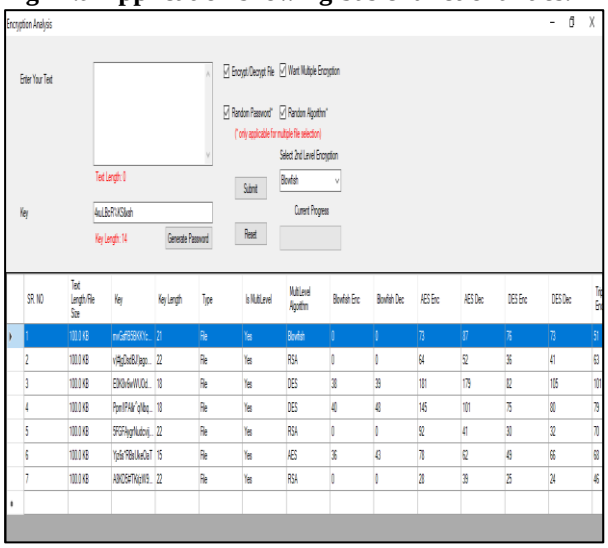

Fig 11.b showing various files encryption time with various multilevel options

Here, the application takes one or many files at a time for encryption and decryption purpose. The facility to provide text instead of a file is also given in the application. This application creates a random secret key/password. For multilevel encryption purpose, a checkbox is given. Here for research purpose, we have taken second level encryption/decryption with RSA algorithm only.

Here we have taken 4 types of files; they are 100KB, 1 MB, 10MB, and 100MB. We have taken 100 files of each type for analysis purpose. We have done the repeated analysis for these files and came to the conclusion.

Analysis:

1. Encryption Time

a. For Single Encryption:

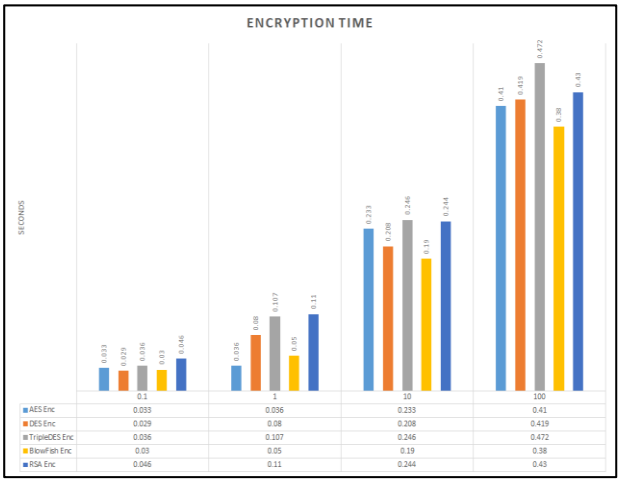

Fig 12.a: Encryption time required for different cryptographic algorithms in msec

b. For Multilevel Encryption:

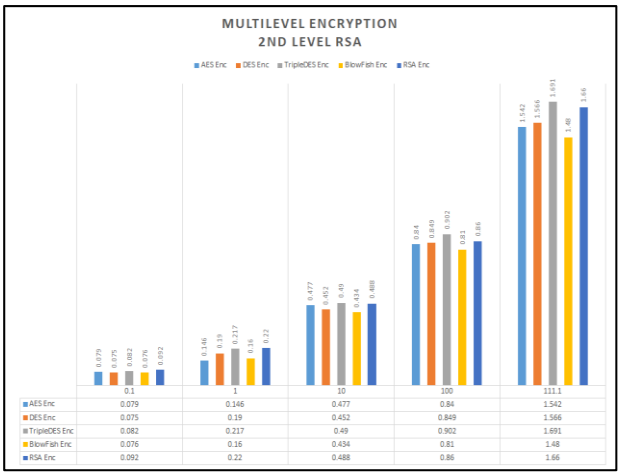

Fig 12.b: Encryption time for multilevel cryptographic algorithm (RSA 2nd level)

2. Decryption time:

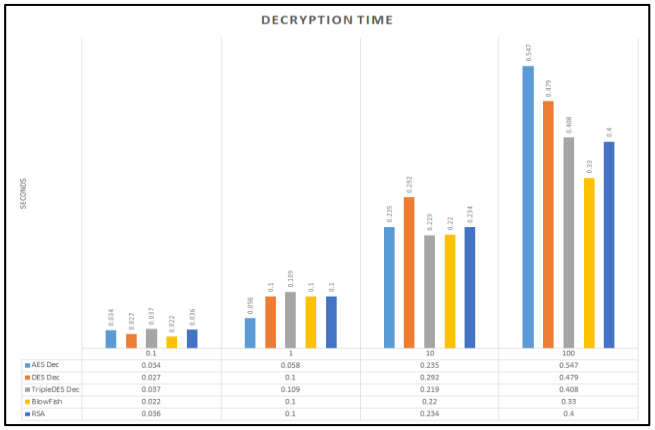

Fig 13.a: Decryption time required for different cryptographic algorithms in msec

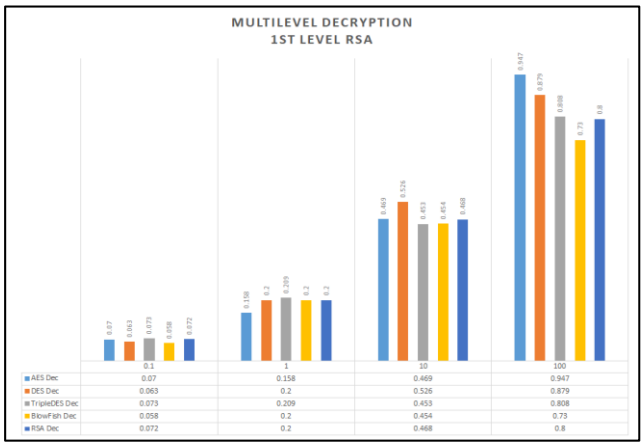

Fig 13.b: Decryption time for multilevel cryptographic algorithm (RSA 1st level)

3. Memory Used

Fig 14: Memory used for different algorithms

4. Throughput:

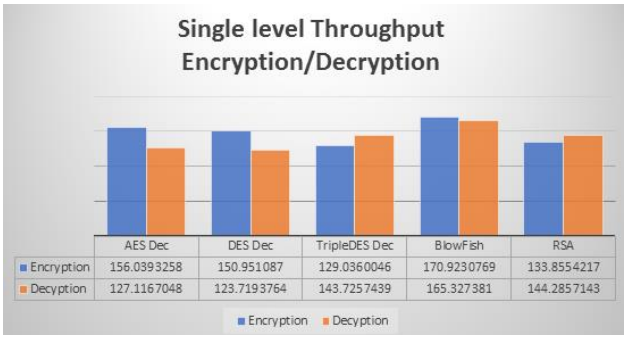

Fig 15.a: Single Level throughput (Encryption/ Decryption)

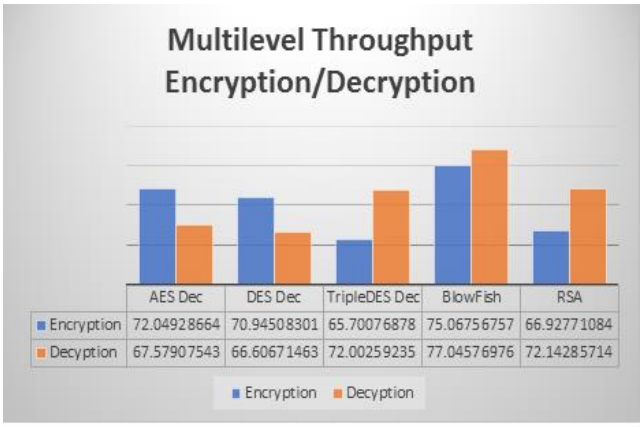

Fig 15.b: Multilevel throughput (Encryption/ Decryption)

Results:

From the analysis done using the application, we have observed that symmetric algorithms are faster than asymmetric algorithms. From the encryption and decryption time for the single cryptographic algorithm, we can summarise that Blowfish is the fastest algorithm amongst symmetric algorithms and then the AES, RSA is the Slowest amongst all.

We have also seen that there is an inverse proportion relation seen between the time taken for encryption and decryption and size of the file. The time taken for encryption and decryption decreases substantially as the file size increases

According to the memory used figure above, we can observe that Blowfish uses least memory, then AES and RSA takes the maximum amount of memory for the execution purpose

Throughput can also be seen as the speed of encryption/decryption done. According to various researchers, as the throughput increases the power consumption for that encryption algorithm decreases.

From this theory, we can observe that Blowfish gave the highest throughput and later AES gave the best results.

When we check the security of these algorithms, AES and blowfish are most promising algorithms because of their key size variations. RSA is the best among asymmetric ones

Conclusion:

Cloud computing has been seen as a revolutionary transformation from buy-as-you-need to pay-as-you-use of IT resources. Many organizations have adopted this huge paradigm shift but still, the cloud industry is seeing a little hesitation in adopting Cloud technology. Security is the prominent barrier. Encryption algorithms that can be used in the cloud computing for confidentiality purpose. Here in this paper, a complete analysis of various crypto-graphical algorithms has done. If the application demands quicker response time then one should use Blowfish Algorithm. If the application demands lesser memory space then one should opt Blowfish / AES algorithm. If an application requires more security AES and Blowfish are major considerations. If Applications need more security then for 2nd level of encryption RSA if the best algorithm.

References:

[1] Cloud Computing Trends: 2017 State of the Cloud Survey, Kim Weins, https://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2017-state-cloud-survey accessed on 09/12/17 at 6:00 pm

[2] Prof. (Ms.) Kimaya Ambekar, Prof. (Dr.) Kamatchi R.Enhanced User Authentication Model in Cloud Computing Security, Springer International Publishing AG 2016, DOI 10.1007/978-3-319-47952-1_26, pg 327-338

[3] Infotechno- Technology is a life, http://www.infotechno.net/cryptography, Accessed on 09/12/17 at 6:00 pm

[4] What is symmetric key encryption?, https://www.quora.com/What-is-symmetric-key-encryption, Accessed on 09/12/17 at 6:00 pm

[5] Giuseppe, Asymmetric RSA encryption in Java, http://www.giuseppeurso.eu/en/asymmetric-rsa-encryption-in-java/, Accessed on 09/12/17 at 6:00 pm

[6]Symmetric-key algorithm, https://en.wikipedia.org/wiki/Symmetric-key_algorithm

[7] Advantages and Disadvantages of Asymmetric and Symmetric Cryptosystems, http://www.uobabylon.edu.iq/eprints/paper_1_2264_649.pdf, Accessed on 09/12/17 at 7:00 pm

[8] Data Encryption Standard, https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm

[9] Ritu Tripathi, Sanjay Agrawal, Comparative Study of Symmetric and Asymmetric Cryptography Techniques, International Journal of Advance Foundation and Research in Computer (IJAFRC), Volume 1, Issue 6, June 2014, ISSN 2348 - 4853

[10] Data Encryption Standard (DES), http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard

[11] Triple DES, https://www.tutorialspoint.com/cryptography/triple_des.htm

[12] Advanced Encryption Standard, https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

[13] Al Jeeva et all, Comparative analysis of performance efficiency and security measures of some encryption algorithms, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248 - 9622 www.ijera.com, Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037

[14] Advanced Encryption Standard (AES),http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard,Accessed on 11/12/17 at 3:00 pm

[15] Diffie–Hellman key exchange, https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange, Accessed on 12/12/17 at 3:00 pm

[16] RSA (cryptosystem), https://en.wikipedia.org/wiki/RSA_(cryptosystem),Accessed on 12/12/17 at 5:00 pm

[17] RSA Public Key Encryption System, https://globlib4u.wordpress.com/2013/10/16/rsa-public-key-encryption-system/, http://www.lsi-contest.com/2008/spec2_e.html#intro, Accessed on 15/12/17 at 2.00pm

