International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 01 | Jan 2022 www.irjet.net p-ISSN: 2395-0072

# Execution Analysis of Different Cryptographic Encryption Algorithms on Different File Sizes on the Cloud and Off the Cloud

**Viswanath Matukumalli[1], Hariharan Seelam[2],Sai Gowtham Inturi[3], Dr. Vijay Babu Burra[4]**

*[1]Under Graduate Student, KL Educational Foundation, Vaddeswaram, Andhra Pradesh*
*[2]Under Graduate Student, KL Educational Foundation, Vaddeswaram, Andhra Pradesh*
*[3]Under Graduate Student, KL Educational Foundation, Vaddeswaram, Andhra Pradesh*
*[4]Professor, KL Educational Foundation, Vaddeswaram Andhra Pradesh*

---

**Abstract-** *Encryption is the process of encoding data to the scrambled or encrypted form. It is generally used to protect sensitive information so that intruders cannot steal it. Encryption means not only changing the plaintext to ciphertext but also includes files and storage devices, as well as the data transferred over wireless networks and the Internet. Nowadays, Cyberpunks are striving too hard to steal the data either from our electronic devices or the data transmitted by us via the Internet. There are many cryptographic methods to defend the attacks of the cyberpunks. Out of these methods which method to be chosen depends on the application demands such as the bandwidth, confidentiality of data, integrity, and response time. In this paper, we have some exciting analysis of the comparison between encryption algorithms over AES, DES, and Blowfish on the cloud and off the cloud.*

***Key Words:*** AES, DES, Blowfish, Data Security, Cryptography, Encryption, Encryption Algorithms, Encryption time, On the cloud, Off the cloud

## 1. INTRODUCTION

Nowadays Cyber thieves are faster, sneakier, and more creative. In 2014 the report of Internet Security teams at Symantec (SYMC) and Verizon (VZ) gives a disturbing image of how troublesome it is turning out for PC clients and Mobile Clients to remain safe on the web. The report says that 317 million new bits of malware which are either PC viruses or malicious software was created in 2014. That implies almost one million new dangers were discharged every day. According to the latest survey of the Symantec (SYMC), the number of attack groups using destructive malware has been raised to 25%.

But at present the evolution of technology and enhancements on the internet makes everyone go digital for banking services, emailing, sending confidential data. Clients store their data in the cloud. To ensure the safety and privacy of the stored data in the cloud, Cryptography, one of the best methods, is used. In cryptography, several operations are present such as encryption, decryption, generation of the signature, or verification of the signature. In cryptography, the data which is stored by the user will be combined with the client specified secret phrase (key) to create an encoded output that is tougher to decode the user stored data without the client specified secret phrase(key).

In this cryptography, the process of encoding the user data with a key to make it as ciphertext is known as Encryption. Encryption of user data will be done through the encryption algorithms. The encryption algorithms are segregated into two types namely Symmetric and Asymmetric encryption algorithms. They are segregated based on the number of keys used to perform the cryptography. If the algorithm uses a single key namely a secret key to perform both encryption and decryption then it comes under the Symmetric Encryption Algorithm. Some of the Symmetric Encryption Algorithms are Advanced Encryption Standard (AES), Data Encryption Standard (DES), triple-DES (3DES), and Blowfish. If the algorithm uses two keys namely public key and private key where the public key is used to perform encryption and the private key is used to perform the decryption then it comes under the Asymmetric Encryption Algorithm. Some of the Asymmetric Encryption Algorithms are ELGAMAL Schema and RSA. Symmetric Encryption Algorithms encrypt the data extremely quickly in secured communication.[1][2][4][5]

Encryption can be done either in the cloud or off the cloud. Encryption on the cloud is faster than off cloud, the performance level of encryption will be high on cloud than off cloud, but encryption on the cloud has its own disadvantages, some cloud providers may not so trustworthy if we encrypt our data in the cloud, keys will also be placed in the cloud, so if in case cloud gets hacked then hacker not only contains encrypted data but also the key which we have used to encrypt data, which is very dangerous as a hacker can easily decrypt data. So, encrypting data in our system and uploading on cloud is much more secured than encrypting in the cloud itself, but nowadays there are many trustworthy cloud providing companies where we can encrypt data in the cloud itself without any worries, this increases the performance of encryption algorithm [1][2][5]

In this paper, our objective is to provide an idea of the encryption time difference of the data between on the cloud and off the cloud using some of the renowned algorithms such as AES, DES, and Blowfish Algorithms.

## 2. LITERATURE REVIEW

Mohammed Nazesh in [1] has analyzed symmetric key encryption algorithms such as RSA, DES, AES,3DES, and Blowfish to prevent the guessing attacks and they concluded that among all the algorithms blowfish and AES requires less time. Devandrasinh Vashi in [2] has analyzed two Algorithms RSA and DES, based on the experimental results he concluded that the DES algorithm requires less encryption time than RSA. Jawahar Thakur in [4] has proposed that Blowfish has better performance results and weak security points when compared with AES and DES. Youssouf Mahamat in [5] has made a comparison between four most common symmetric key encryption algorithms: AES, DES, Blowfish and Cast 128 and concluded that AES gives the best security among these four algorithms. Kuntal Patel in [6] has analyzed the most 3 common Symmetric encryption algorithms AES, DES, Blowfish and based on the performance results he concluded that Blowfish is better than AES and DES based on memory requirements during execution. Hence for memory constraint applications, use of Blowfish should be advisable for security implementation.

## 3. RELATED WORK

Cloud Storage Delivery models are mainly three kinds namely public cloud, private cloud, hybrid cloud, and community cloud. [8]

In Public Cloud, cloud services are open to the public and can be utilized by anyone. The cloud assets such as storage and service will be possessed and operated by the cloud service provider. The public cloud is commonly utilized to offer web-based emails, online applications, storage, and for own development conditions. [8]

In a private cloud, cloud services are utilized by a single organization or business corporation to fit its resources, applications to meet their needs and requirements for their specific development. Security for the data is high and has a flexible cloud environment such that the organization can organize its cloud environment. The Private cloud will not be shared with anyone else other than the organization.[8]

In the Hybrid cloud, the name itself gives an idea of the combination of two cloud services both private and public clouds. In the Hybrid cloud, a company or organization utilizes both private cloud and public cloud such that it can have both advantages of public and private cloud. Private cloud is utilized for highly confidential data and public cloud is utilized to perform operations on huge data which is of less sensitivity.[8]

In the Community cloud, some group of organizations which are having the same concerns and requirements shares the cloud services. Community cloud will be organized by the organizations which share the cloud services. In the community cloud also there will be both public cloud and private cloud advantages such as cost will be reduced as the infrastructure bill will be distributed, privacy level, and policy agreement.[8]

## 4. PROPOSED MODEL

Encryption Algorithms chose for analysis

i. DES (Data Encryption Standard) Algorithm
ii. AES (Advanced Encryption Standard) Algorithm
iii. Blowfish Encryption Algorithm

### DES (Data Encryption Standard) Algorithm:

DES (Data Encryption Standard) algorithm helps to encrypt the digital data stored in the cloud. It belongs to the Symmetric Encryption Algorithm. It was created during the early 1970s by IBM. It was later embraced by the National Institute of Standards and Technology (NIST). The US government's first foremost approved encryption algorithm was DES which is the main reason to get embraced quickly by the organizations, industries where the demand for encryption is high. The straightforwardness of DES made the companies based on embedded systems, SIM cards, routers, set-top boxes, and modems to utilize it to a great extent.[1]

DES (Data Encryption Standard) Algorithm is a block cipher algorithm. DES converts the user input data to ciphertext by dividing the data into blocks of size 8 bytes i.e. 64 bits using a secret key of size 7 bytes i.e. 56 bits. In DES, the same key will be used for both encrypting the user input data to ciphertext and decrypting the ciphertext to user data. Hackers must go through 2^56 possibilities at maximum to discover the matching key to decrypt the ciphertext. DES depends on the two crucial characteristics of cryptography: substitution (also known as confusion) and transposition (also known as diffusion). DES totally performs 16 rounds of encryption to encode the plaintext into ciphertext.[1][4]

In DES, the plain text will be divided into 64 bits blocks and will be sent over to initial Permutation function to perform the initial permutation function over the plain text block and next permuted block will be divided into two splits namely Left Plain Text (LPT) and Right Plain Text (RPT). Now both LPT and RPT will be encrypted by 16 rounds of encryption. This encoded LPT and RPT will be joined again to run under Final Permutation (FP) to get the final output.[1][4]

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

AES (Advanced Encryption Standard) Algorithm is one of the renowned algorithms in the encryption of electronic data in the cloud. It belongs to the same symmetric encryption algorithm. AES is designed by Vincent Rijmen and Joan Daemen. So, DES is also called Rijndael which comes after their names. AES overtakes the position of DES by being embraced by the US government in 2001 and it is being utilized worldwide. AES is intended to apply easily in both hardware and software, and as well as in prohibited environments, for instance, smart cards and can defend the attacks by cyberpunks in a very decent manner.

AES (Advanced Encryption Standard) Algorithm is a block cipher algorithm. AES comprises three block ciphers namely AES-128, AES-192, and AES-256. AES-128 uses the key of length 128 bits i.e. 16 bytes to encrypt and decrypt a block of data and 10 rounds of encryption take place for encrypting the plain text. AES-192 uses the key of length 192 bits i.e. 24 bytes to encrypt and decrypt a block of data and 12 rounds of encryption take place for encrypting the plain text. AES-256 uses the key of length 256 bits i.e. 32 bytes to encrypt and decrypt a block of data and 10 rounds of encryption take place for encrypting the plain text.

AES divides the data block of size 128 bits into four blocks. Those blocks are considered as an array and organized as a matrix of dimension 4 x 4. That matrix is termed as State. The Encryption starts with the AddRoundKey Stage in which every byte that belongs to that state will be performed the bitwise-xor operation with the round key block. Next to that four processes will be processed for 9 rounds, 11 rounds, and 13 rounds for AES-128, AES-192, and AES-256 respectively. Those four processes are

(i) **SubBytes process** in which each byte is substituted with another byte corresponding to the lookup table or Rijndael Xbox.
(ii) **ShiftRows process** in which the last three rows of the state are altered in a cyclic manner for a specific number of moves.
(iii) **MixColumns process** in which four bytes of each column are combined or mixed.
(iv) **AddRoundKey process** in which every byte that belongs to the state will be performed the bitwise-xor operation with a round key block.

In the final round, the MixColumns process will be exempted and the remaining three processes will be processed which provides the encrypted data i.e. ciphertext.

**Blowfish Algorithm:**

Blowfish Algorithm is an encrypting algorithm that encrypts the data in the cloud faster than the DES algorithm. The blowfish algorithm also comes under the Symmetric Encrypting Algorithms. Bruce Schneier designed this algorithm in the year 1993. It was designed as an alternative for the DES algorithm. Blowfish algorithm is license-free and available in the public domain which can be used by everyone. [5]

Blowfish Algorithm is a block cipher algorithm. It divides the text into blocks of size of 64 bits. In the Blowfish algorithm, key length varies from 32 bits to 448 bits. Encryption will be done for 16 rounds. Four S-boxes (Substitution boxes) will be present in the Blowfish Algorithm. [1][4][5]

In the Blowfish algorithm, 18 subkeys are necessary for both encryption and decryption processes. These 18 subkeys are arranged in an array initialized with 32-bit subkeys in hexadecimal format. Bitwise XOR operation will be performed between the P[i] (i refers to the iteration which values iterates from 0 to 17) and $i^{th}$ 32-bits of the key. For instance, (P[1]) xor ($1^{st}$ 32 bits of the key), etc. After the result will be stored back in P[i]. The newly updated values in the P-array are 18 subkeys used to encrypt the user data to ciphertext. Encryption of user data in the Blowfish Algorithm is followed by two stages. Initially, the round function should be iterated for 16 times. In which 64-bit input will be made into two half blocks of size 32 bits each namely L and R. Perform XOR operation to the Left part L with P[i] in every $i^{th}$ iteration and output will be inputted for a Function F in which the function is divided into 4 S-boxes S1, S2, S3, and S4 respectively. The input of size 32 bits is divided into 4 parts i.e. 8 bits each and inputted for each S-box which outputs the 8-bit input to 32 bits. The output of S1 and S2 will undergo an additional operation. The added result of S1 and S2 and output of S3 will undergo XOR operation. The result of XOR operation and output of S4 will undergo addition and gives the final output from the function. The output from the function and Right part R of input plain text will undergo XOR operation. Now the output of XOR operation between Left part L and P[i] and the output of XOR operation of Right part R and Function F will be swapped. This whole process will be repeated for 16 rounds of iterations in which revised subkeys from P[1] to P[16] are used. After 16 iterations, revoke the last swap performed in $16^{th}$ iteration. Perform the XOR operation between L and P[18] to get the Left ciphertext. Perform XOR operation between R and P[17 ] to get the Right ciphertext.

**5. EXPERIMENTAL SETUP**

Experiments are performed to examine the difference between the time for encryption of data on the cloud and

time for encryption of data off the cloud using AES, DES, and Blowfish Algorithms.

Experiments have been executed in Java Programming language. Five programs namely DESEncry.java, AESEncry.java, BlowishEncry.java, encryptionchooser.java, index.jsp have been built and run to trace the encryption time difference. Execution is done for five distinct files of various sizes.

Each program is being executed for five times to ensure consistency and accuracy of results to evaluate the precise encryption time. All the results are recorded after the execution of the program. The average of the five records is considered and evaluated the time difference.

### 5.1 Experimental environment

**Hardware used for Research:**

- Processor: Intel Core i3 7th Gen 7020U
- Clock Speed: 2.3 GHz
- RAM Installed: 4 GB DDR4(3.10 utilizable)

**Software used for the Research:**

- System type: 64-bit Operating System
- Operating System (OS): Windows 10 Home Single Language
- Java Platform: Eclipse IDE 2019
- Server: Apache Tomcat 8.5.56

### 5.2 Experimented Data Files and File Size

For Research and Analysis, a total five number of files of various sizes of 100KB, 500KB, 1MB, 2MB, and 5MB have experimented. Average Encryption time is recorded for each file by each algorithm and represented in tables 1, 2, and 3 respectively. Average time comparison for encrypting the data on the cloud and off the cloud using DES, AES, and Blowfish algorithms are recorded in tables 4, 5, and 6 respectively.

## 6. RESULT ANALYSIS OF EXPERIMENTS:

In this section, the analysis of the results obtained after the experiment is visualized through the graphical representation.

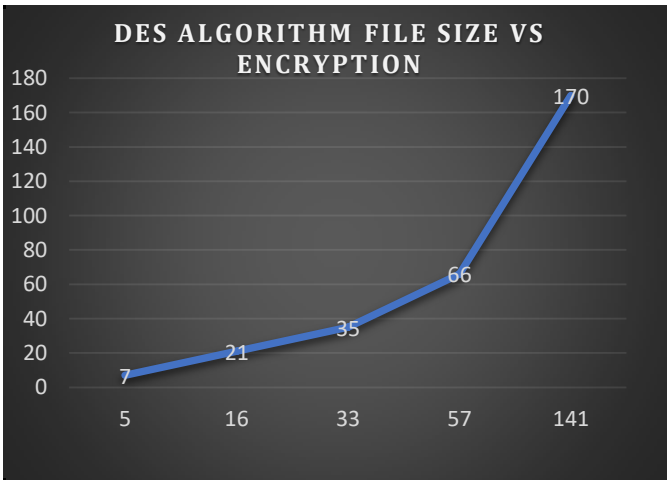
### 6.1 Performance of Data Encryption Standard (DES) Algorithm on five different files varied by size based on Encryption time

DES ALGORITHM FILE SIZE VS ENCRYPTION TIME COMPARATIVE STUDY

**Table-6.1**

| FILE SIZE | AVERAGE TIME | ATTEMPTS TIME(ms) | |
|---|---|---|---|
| 100 KB | 7 | 1 | 7 |
| | | 2 | 8 |
| | | 3 | 6 |
| | | 4 | 7 |
| | | 5 | 8 |
| | | AVERAGE | 7 |
| 500 KB | 21 | 1 | 19 |
| | | 2 | 21 |
| | | 3 | 23 |
| | | 4 | 18 |
| | | 5 | 26 |
| | | AVERAGE | 21 |
| 1 MB | 35 | 1 | 38 |
| | | 2 | 36 |
| | | 3 | 35 |
| | | 4 | 35 |
| | | 5 | 32 |
| | | AVERAGE | 35 |
| 2 MB | 66 | 1 | 60 |
| | | 2 | 69 |
| | | 3 | 75 |
| | | 4 | 64 |
| | | 5 | 65 |
| | | AVERAGE | 66 |
| 5 MB | 170 | 1 | 166 |
| | | 2 | 175 |
| | | 3 | 165 |
| | | 4 | 175 |
| | | 5 | 170 |
| | | AVERAGE | 170 |

**Graph-6.1**



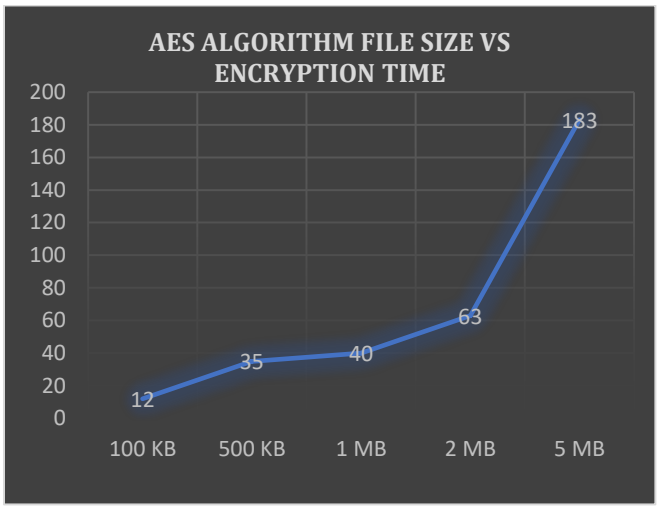
### 6.2 Performance of Advanced Encryption Standard (AES) Algorithm on five different files varied by size based on Encryption time

AES ALGORITHM FILE SIZE VS ENCRYPTION TIME COMPARATIVE STUDY

**Table-6.2**

| FILE SIZE | AVERAGE TIME | ATTEMPTS TIME(ms) | |
|---|---|---|---|
| 100 KB | 12 | 1 | 9 |
| | | 2 | 7 |
| | | 3 | 11 |
| | | 4 | 12 |
| | | 5 | 11 |
| | | AVERAGE | 12 |
| 500 KB | 35 | 1 | 42 |
| | | 2 | 42 |
| | | 3 | 21 |
| | | 4 | 36 |
| | | 5 | 34 |
| | | AVERAGE | 35 |
| 1 MB | 40 | 1 | 42 |
| | | 2 | 38 |
| | | 3 | 35 |
| | | 4 | 42 |
| | | 5 | 43 |
| | | AVERAGE | 40 |
| 2 MB | 63 | 1 | 73 |
| | | 2 | 63 |
| | | 3 | 60 |
| | | 4 | 66 |
| | | 5 | 52 |
| | | AVERAGE | 63 |
| 5 MB | 183 | 1 | 144 |
| | | 2 | 206 |
| | | 3 | 161 |
| | | 4 | 200 |
| | | 5 | 204 |
| | | AVERAGE | 183 |

**Graph-6.2**




### 6.3 Performance of Blowfish Algorithm on five different files varied by size based on Encryption time

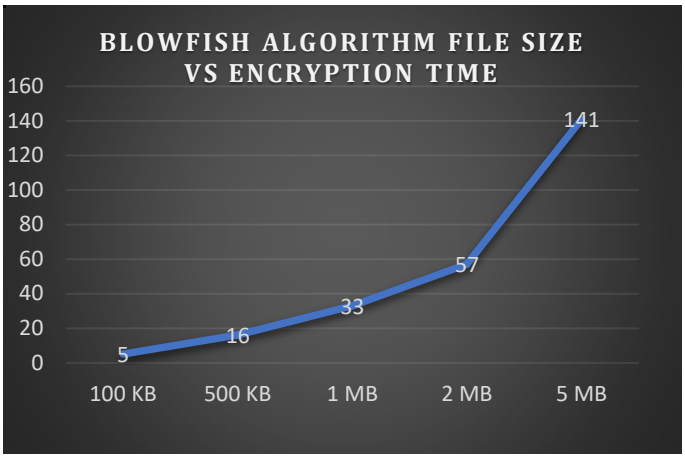
BLOWFISH ALGORITHM FILE SIZE VS ENCRYPTION TIME COMPARATIVE STUDY

**Table-6.3**

| FILE SIZE | AVERAGE TIME | ATTEMPTS TIME(ms) | |
|---|---|---|---|
| 100 KB | 5 | 1 | 6 |
| | | 2 | 6 |
| | | 3 | 6 |
| | | 4 | 5 |
| | | 5 | 6 |
| | | AVERAGE | 5 |
| 500 KB | 16 | 1 | 16 |
| | | 2 | 17 |
| | | 3 | 18 |
| | | 4 | 17 |
| | | 5 | 16 |
| | | AVERAGE | 16 |
| 1 MB | 33 | 1 | 29 |
| | | 2 | 31 |
| | | 3 | 23 |
| | | 4 | 30 |
| | | 5 | 28 |
| | | AVERAGE | 25 |
| 2 MB | 57 | 1 | 59 |
| | | 2 | 60 |
| | | 3 | 58 |
| | | 4 | 57 |
| | | 5 | 55 |
| | | AVERAGE | 57 |
| | | 1 | 143 |
| | | 2 | 138 |
| | | 3 | 143 |

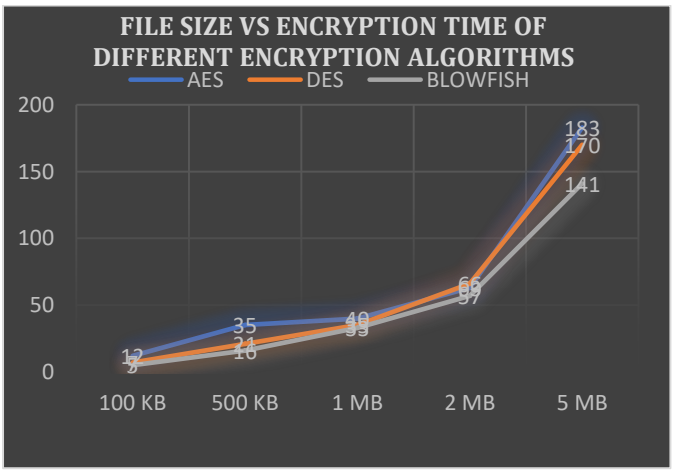
| | | | |
|---|---|---|---|
| 5 MB | 141 | 4 | 142 |
| | | 5 | 139 |
| | | AVERAGE | 141 |

**Graph-6.3**




**6.4 Performance of DES, AES, and Blowfish Algorithms on five different files of different sizes based on Encryption time on Cloud**

**Graph-6.4**



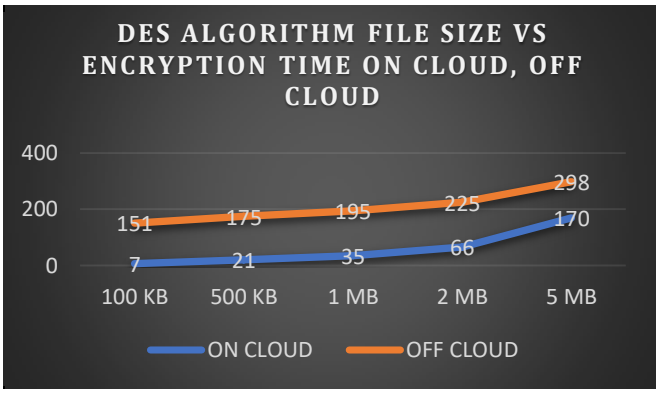

**6.5 Performance of DES algorithm based on Encryption time on cloud vs off cloud**

DES ALGORITHM FILE SIZE VS ENCRYPTION TIME ON CLOUD, OFF CLOUD

**Table-6.5**

| TYPE | FILE SIZE | TIME TAKEN(ms) |
|---|---|---|
| OFF CLOUD | 100 KB | 151 |
| | 500 KB | 175 |
| | 1 MB | 195 |
| | 2 MB | 225 |
| | 5 MB | 298 |
| ON CLOUD | 100 KB | 7 |
| | 500 KB | 21 |
| | 1 MB | 35 |
| | 2 MB | 66 |
| | 5 MB | 170 |

**Graph-6.5**



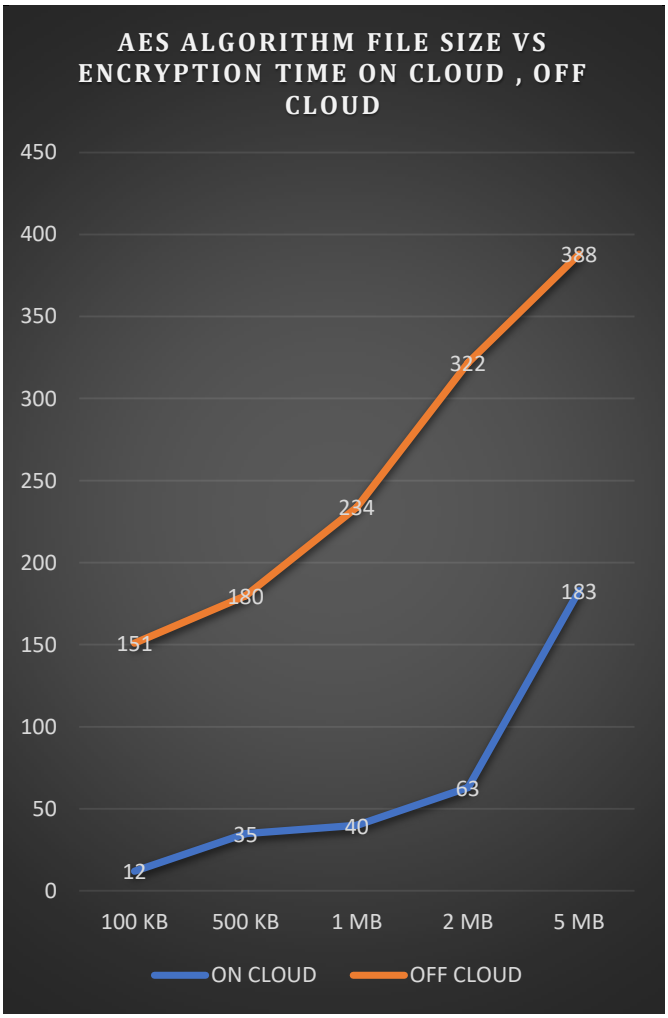

**6.6 Performance of AES algorithm based on Encryption time on cloud vs off cloud**

AES ALGORITHM FILE SIZE VS ENCRYPTION TIME ON CLOUD, OFF CLOUD

**Table-6.6**

| TYPE | FILE SIZE | TIME TAKEN(ms) |
|---|---|---|
| OFF CLOUD | 100 KB | 151 |
| | 500 KB | 180 |
| | 1 MB | 234 |
| | 2 MB | 322 |
| | 5 MB | 388 |
| ON CLOUD | 100 KB | 12 |
| | 500 KB | 35 |
| | 1 MB | 40 |
| | 2 MB | 63 |
| | 5 MB | 183 |

**Graph-6.6**



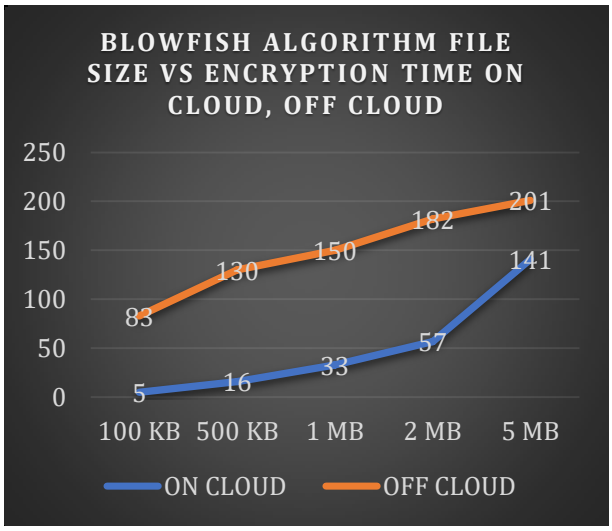

### 6.7 Performance of Blowfish algorithm based on Encryption time on cloud vs off cloud

BLOWFISH ALGORITHM FILE SIZE VS ENCRYPTION TIME ON CLOUD, OFF CLOUD

**Table-6.7**

| TYPE | FILE SIZE | TIME TAKEN(ms) |
|---|---|---|
| OFF CLOUD | 100 KB | 83 |
| | 500 KB | 130 |
| | 1 MB | 150 |
| | 2 MB | 182 |
| | 5 MB | 201 |
| ON CLOUD | 100 KB | 5 |
| | 500 KB | 16 |
| | 1 MB | 33 |
| | 2 MB | 57 |
| | 5 MB | 141 |

**Graph-6.7**




## 7. OUTCOMES AND USAGE OF EXPERIMENTAL RESULTS

Experimental results on DES, AES and Blowfish Algorithms execution on five different files of variant sizes provides an explicit indication of observations stated in 5.1

### 7.1 Performance analysis of AES, DES, and Blowfish for encryption time

Based on the results of the experiment, the Blowfish algorithm is faster than AES and DES algorithms. Encryption of data on the cloud is faster than the encryption of data off the cloud. So, encrypting the data on the cloud increases the performance of the algorithm. [1][4][5]

### 7.2 Usage of Experimental results

With the results of the experiment, one can analyze which algorithm performs better in a given circumstance. It also gives intelligibility about the performance of an algorithm on the cloud and the execution of the algorithm away from the cloud. With these results, one can make encryption of data more perfectly, can make to get the most performing algorithm in given conditions among all available algorithms

## 8. CONCLUSION

A literature review provides an idea that DES, AES, and Blowfish are all well-known algorithms for encryption of data in the cloud. The experimental result demonstrates that the performance of the Blowfish Algorithm is better than DES and AES based on the encryption time of data on the cloud. Encryption of the data on the cloud takes lesser time than the encryption of the data away from the cloud.

## 9. FUTURE REFERENCE

This paper evaluates the performance of DES, AES, and Blowfish algorithm based on encryption time on files of size up to 5 MB and the difference between encryption time of data on cloud and encryption time of data off cloud. This research will be further proceeded to compare the performance of the above algorithms on files of size more than 5 MB and to evaluate the encryption time difference between Asymmetric Encryption algorithms on cloud and off the cloud.

## REFERENCES

1. Nazeh Abdul Wahid MD, Ali A, Esparham B, Marwan MD (2018) A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention. J Comp Sci Appl Inform Technol. 3(2): 1-7. DOI: 10.15226/2474-9257/3/2/00132
2. Patel, K. (2019). Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files. International Journal of Information Technology. doi:10.1007/s41870-018-0271-4
3. Youssouf Mahamat, Siti Hajar Othman, Herve Nkiama (2016) Comparative Study Of AES, Blowfish, CAST-128 And DES Encryption Algorithm DOI:10.9790/3021-066010107
4. Jawahar Thakur, Nagesh Kumar DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance
5. Analysis (ISSN 2250-2459, Volume 1, Issue 2, December 2011)
6. Priyadarshini P, Prashant N, Narayan DG, Meena SM. A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. Procedia Computer Science. 2016;78:617-624.
7. Mohammed, Abdalbasit & Varol, Nurhayat. (2019). A Review Paper on Cryptography. 1-6. 10.1109/ISDFS.2019.8757514.
8. Stallings W (2005) Cryptography and network security principles and practices. 4th edn. Prentice Hall of India, India
9. Prasad, M.Rajendra & Naik, R Lakshman & V, Dr. Bapuji. (2013). Cloud Computing : Research Issues and Implications. International Journal of Cloud Computing and Services Science. 2. 134-140. 10.11591/closer.v2i2.1963.
10. Yogesh K, Rajiv M, Harsh S. Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures. International Journal of Computer Science and Management Studies. 2011;11(3):60-63.
11. Jeeva AL, Palanisamy V, Kanagaram K. Comparative analysis of performance efficiency and security measures of some encryption algorithms. International Journal of Engineering
12. Research and Applications. 2012;2(3): 3033-3037.
13. Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures byYogesh Kumar, Rajiv Munjal, and Harsh ,(IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 – 4853
14. Ritu T, Sanjay A. Comparative Study of Symmetric and Asymmetric Cryptography Techniques. International Journal of Advance Foundation and Research in Computer. 2014;1(6):68-76.
15. Comparative analysis of performance efficiency and security measures of some encryption algorithms by AL. Jeeva, Dr. V. Palanisamy, K. Kanagaram compares symmetric and asymmetric cryptography algorithms ISSN: 2248-9622
16. Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength Against Attacks."I BM Journal of Research and Development, May 1994, pp. 243 -250.
17. Xin Z, Xiaofei T. Research and Implementation of RSA Algorithm for Encryption and Decryption. 6th International Forum on Strategic Technology. 2011:1118-1121.
18. Bono SC, Green M, Stubblefield A, Juels A, Rubin AD, Szydlo M. Security analysis of a cryptographically-enabled RFID device. In:
19. SSYM'05: Proceedings of the 14thconference on USENIX Security Symposium. 2005.
20. Pooja B. Optimization of Cryptography Algorithms in Cloud Computing. International Journal of Computer Trends and Technology. 2017;46(2):67-72.
21. Shraddha D. Performance Analysis of AES and DES Cryptographic Algorithms on Windows & Ubuntu using Java. International Journal of Computer Trends and Technology. 2016;35(4):179-183.
22. Polimon J, Hernandez-Castro JC, Estevez-Tapiador JM, Ribagorda A. Automated design of a lightweight block cipher with genetic programming. Int J Know-Based Intell Eng Syst. 2008;12(1):3-14.
23. Pratap CM. Superiority of blowfish Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering. 2012;2(9):196-201.
24. Sonal S, Prashant S, Ravi Shankar D. RSA algorithm using modified subset sum cryptosystem. 2nd International Conference on Computer and Communication Technology. 2011:457-461.