# Performance Comparison of Cryptographic Algorithms for Data Security in Cloud Computing

Mr.Srinu Banothu[1]
Research Scholar, JNTUH,
Assistant Professor, Dept of CSE,
Vignan Institute of Technology and Science
Hyderabad, India
Email: srinub1307@gmail.com

Dr. A. Govardhan[2]
Professor & Rector
Dept. of CSE, JNTUH
Hyderabad, India
email: govardhan_cse@yahoo.com

Dr. Karnam Madhavi[3]
Professor, Dept of CSE,
GRIET, Hyderabad, India
Email: bmadhaviranjan@yahoo.com

## *Abstract*

*Cloud computing is a trending technology used to provide on-demand computing, and data storage services through the internet to organizations, enterprises, and individuals. The users of cloud computing can access cloud services from anywhere, anytime by connecting their device to the internet. One of the cloud services is Data storage as a service (DaaS), through which, the user can outsource their huge amount of data to the cloud environment, to reduce the cost of establishing the infrastructure locally and maintenance. But the biggest challenge is the security of outsourced data because the cloud service provider is not a trusted one and all sensitive data is in the control of the cloud vendor. So to provide security to the data in the cloud, one of the solutions is encryption of data using cryptographic algorithms and outsource to the cloud to provide data confidentiality and privacy. Many authors contributed their work to achieve good data confidentiality and privacy using cryptographic algorithms and evaluated their performances. In our paper, we are presenting the study of various cryptography algorithms and the comparison of the performances of cryptographic algorithms evaluated by various authors on varied file sizes and determining their find outs.*

**Keywords:** Cloud Computing, Cryptography, Data Storage service (DaaS).

## 1 Introduction

Cloud computing is a trending technology used to provide on-demand computing, and data storage services through the internet to organizations, enterprises, and individuals. The users of cloud computing can access cloud services from anywhere, anytime by connecting their device to the internet. Cloud computing provides various services like Platform as a Service(PaaS), Infrastructure as a Service(IaaS), Software as a Service(SaaS). Infrastructure as a Service(IaaS) provides the data storage service, in this, the enterprise, organization, or individual can outsource their data to the cloud environment. The major issues are security to the outsourced data, the vendor may leak the user's sensitive data to unauthorized parties so that the confidentiality of data goes off. To make sure the data is secure at cloud vendors, many authors have given security frameworks in which all these cryptographic algorithms are used. In which the user

encrypts the data to be outsourced with a key and encrypted form of data will be sent to the cloud, then cloud vendor is unaware about the content and data will be confidential. For encrypting the data some authors used symmetric cryptographic algorithms and asymmetric cryptographic algorithms. In our paper, we are presenting the performances evaluated on various algorithms by considering the parameters like encryption time, file type, file size, and security levels and comparison of performances.

## 2. Literature on Cryptographic Algorithms

In most of cloud security algorithms, cryptographic algorithms are used to convert the readable message into an unreadable format using a key known as Encryption. Converting unreadable messages into a readable format known as decryption. There are two categories of Cryptographic Algorithms.

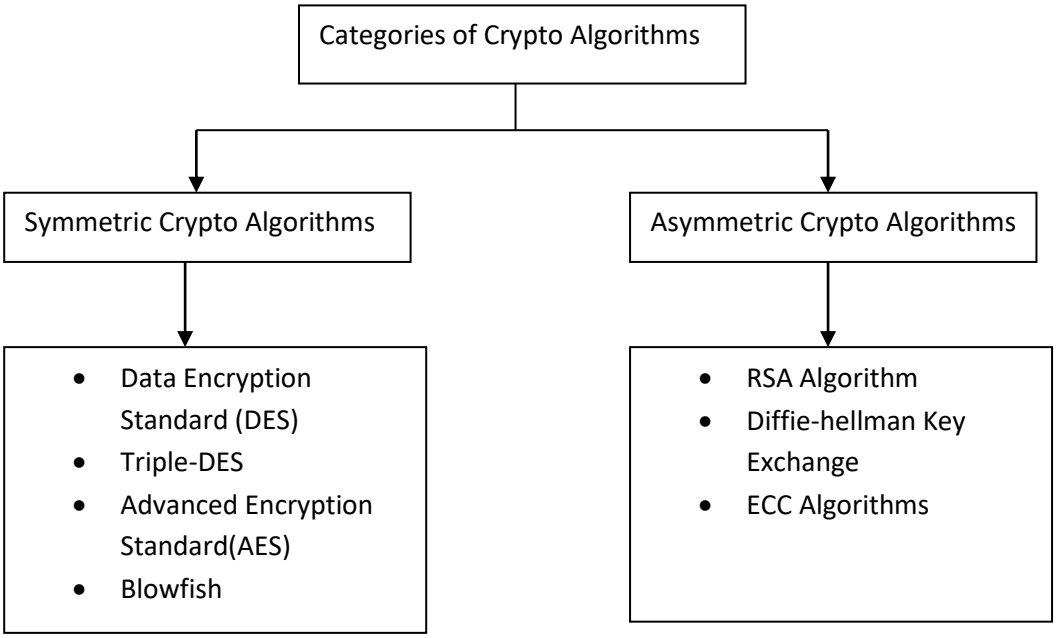


**Figure 1: Categories of Cryptographic Algorithms**

**2.1 Symmetric Crypto Algorithms:** Cryptographic algorithms use the same key for encryption and decryption is known as Symmetric Cryptographic Algorithms

**Data Encryption Standard Algorithm (DES)**:

It is a symmetric block cipher, it converts a plain text block into an equivalent size ciphertext block. DES block size 64bit, Key size is 56 bit. It is based on the Feistel Cipher Structure. DES algorithm structure and its operation.

- Performs the initial permutation(IP) on a 64-bit block of data

- Breaks the input block into two half's(32 bit each)
- Perform substitution on the left half of the data using bitwise XOR operation.
- Performs permutation using round function on subkey and right half of the data
- DES passes through 16 rounds
- Then have final permutation, being the inverse of I**P**
- DES encryption Process is shown in the below figure.

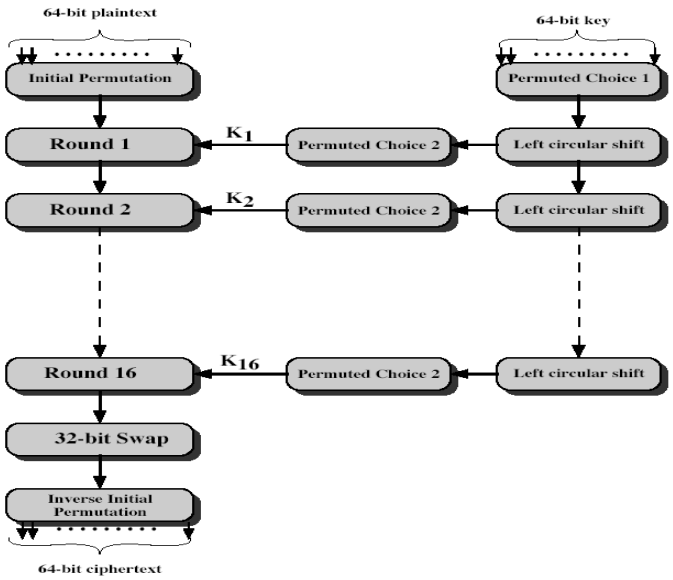


**Figure 2: DES Algorithm Structure**

The advantage of DES is Key size, with 56-bit key, there are $2^{56}$ = 7.2 x 1016 possible values, so brute force attack is impractical. But, DES finally proved that it was insecure in july-1998, because the Electronic Frontier Foundation (EFF) had broken a DES encryption using a special-purpose "DES cracker" machine, and that machine was built for less than $250,000. It has taken less than three days to attack the cipher. An alternative to DES is the triple DES algorithm.

**Triple DES:**

Triple DES is a replacement for single key DES, It needs three keys to encrypt the data because each DES uses a 56-bit key, triple DES uses 3*56=168 bit key, so the brute force attack is impossible with this key size.

Triple-DES with two keys is also a great alternative to single-DES but suffers from being 3 times slower to run. There are no practical attacks; however, there are some indications of attack approaches. Therefore, Triple-DES with three keys is used for greater security.

Encryption: $C = E_{K3}[D_{K2}[E_{K1}[P]]]$

Decryption: $P = D_{k3}[E_{k2}[D_{k1}[C]]]$

**Blowfish:**

Blowfish is a symmetric block cipher invented by Bruce Schneier in 1993 and 94. Blowfish Key Schedule size is from 32 to 448-bit key, used to generate 18, 32-bit sub-keys stored in P-array: P1 to P18, S-boxes are indicated by Si,j, where i=1..4 and j=0..255.

Blowfish Encryption:

- It performs two basic operations: bitwise XOR and Addition
- Data block is partitioned into 2- 32-bit halves L0 & R0

for k = 1 to 16 do

Rk = Lk-1 XOR Pk;

Lk = F[ Rk ] XOR Rk-1;

L17 = R16 XOR P18;

R17 = L16 XOR k17;

Where F[p,q,r,s] = ((S1,p + S2,q) XOR S3,r) + S4,p

Break 32-bit Rk into (p,q,r,s)

Since, provided key is large enough, a brute-force attack is not practical. And the key-dependent S-boxes and sub-keys make analysis very difficult for the given the high key schedule cost. Very few cryptanalysis results on blowfish, changing both halves in every round increases security.

**Advanced Encryption Standard (AES):**

It is also a symmetric block cipher, it uses a data block of 128-bit size to encrypt or decrypt and key sizes are 128,192 and 256 bit.

The plain text data is partitioned into blocks of 128 bit each, and the data block is arranged in a 4x4 matrix form of bytes. Then 1$^{st}$ four bytes of a 128-bit input block are in the first column in the 4 × 4 matrix of bytes. The next four bytes are in the second column, and so on. The state array in AES is represented by the 4×4 matrix of bytes.

The AES algorithm performs four functionalities in each round: Substitute Bytes, shift rows, Mix Columns and Add Round Key

Substitute Bytes: This is a substitution transformation, which is a table lookup using a 16 × 16 matrix of byte values known as s-boxes.

Shift Rows: It is a simple permutation transformation. In this transformation the 1st row of the state array matrix is not altered. – The 2nd row is shifted 1 byte, the 3rd row is shifted 2 bytes, 4th row is shifted 3 bytes to the left in a circular fashion.

Mix Columns: It is a substitution transformation. This transformation is performed by multiplying the state array matrix with identity matrix. Then each column element is replaced by a new value, it is a function of all four elements within the same column.

Add Round Key: It is also a substitution transformation, in which each byte value of resultant matrix is the result of bitwise XOR of each byte of state array matrix and each byte of the 128 bits of the round key. This is a column-wise operation between the 4 bytes of a state column and one word of the round key. This transformation is very simple and provides good efficiency but its drawback is equally of state.

The Encryption or Decryption process starts with an Add round key transformation and process 9 rounds of four functionalities and the tenth round is with 3 functionalities. The decryption process is the inverse of its counterpart within the encryption algorithm.

The AES key expansion takes 4 words key as input and gives a linear array of 44 words. Each round uses 4 words from those 44 words. Each word contains 32 bytes which suggest each sub-key is 128 bits long.

**2.2 Asymmetric Crypto Algorithms:** Cryptographic algorithms use two different keys one for encryption and the other for decryption such algorithms are known as asymmetric Cryptographic Algorithms. The popular asymmetric algorithm is the RSA algorithm.

**RSA Algorithm:**

It is a asymmetric key algorithm, developed by Ron Rivest, Adi Shamir, Len Adelman, both public and private keys are interchangeable, variable Key Size (512, 1024, or 2048 bits), and the Most popular public key algorithm

RSA Key Generation, Encryption, and Decryption:

**Key Generation:**

Choose any two large random prime numbers p & q

Find N=p*q and z=(p-1)*(q-1)

Select a random number e, 1<e<N, GCD(e, z)=1, where 'e' is the public key

Find number d, such that e*d = 1 mod z, 0<=d<=N

Keys are generated using N, d, e

Public key : {N, e}

Private key: {N, d}

**Encryption:** $C = M^e \bmod N$ where M->is plain text and C-> is cipher text

**Decryption:** $M = C^d \bmod N$

The public key can be used for encryption and is shared and the private key is used for decryption, so it hidden.

## 3. Comparison of Cryptographic algorithms performances

**Table 1:Comparison of Existing Work**

| **Authors** | **Work title** | **Performance compared Algorithms** | **File type** | **Find outs** | **Maximum Filesize** | **Security level** |
|---|---|---|---|---|---|---|
| Akashdeep, GVB Subrahmanyamb, Vinay A Hanumat Sastry | Security Algorithms for Cloud Computing | DES,3DES, and AES | Text File | AES is good for key encryption and MD5 is suitable for encoding | 25MB | More secure |
| Murtala Aminu Baba Abdulrahman Yusuf Aminu Ahmad Ladan Maijama'a | Performance Analysis of the Encryption Algorithms as Solution to Cloud Database Security | AES128,192,256 3DES168 | Database | AES128 | 100kb | More secure |
| Erick Fernando Dine Agustin Muhamad Iran | Performance Comparison of Symmetries Encryption Algorithms AES and DES With Raspberry Pi | AES128, DES | message | AES128 | 160kb | More secure |
| Priyadarshini.P, Prashant Narayankar b | Comprehensive Evaluation of Cryptographic | DES, 3DES, AES, RSA, and Blowfish | Text File | AES | 3MB | More secure |

| | | | | | | |
|---|---|---|---|---|---|---|
| ,Narayan D G c , Meena S M | Algorithms: AES, DES, 3DES, RSA, and Blowfish | | | | | |
| Bih-Hwang Lee | Data Security in Cloud Computing Using AES Under HEROKU Cloud | AES | Text File | AES | 15000KB | More secure |

## 4. Conclusion and Future Scope

Data security in the cloud is a major concern since cloud vendors are not trusted parties, to prevent from losing data confidentiality and finding the best security algorithms required to implement a security framework. In this paper discussed about symmetric and asymmetric cryptographic algorithms Performances of those algorithms in terms of encryption time and security level in the cloud environment of varied file sizes are compared and finally, all authors found that AES algorithms are best in terms of encryption time on varying sized files and security levels. My future research is to apply these algorithms for cloud database encryption and find the best cryptographic algorithms for encryption of databases of large size based on encryption time and security level.

## *5. References*


1. *Akashdeep Bhardwaj*, GVB Subrahmanyamb, Vinay Avasthic, Hanumat Sastryd Security Algorithms for Cloud Computing, International Conference on Computational Modeling and Security (CMS 2016)*
2. *Priyadarshini Patila,*, Prashant Narayankarb, Narayan D G c, Meena S MdA Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish, International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA.*
3. *Erick Fernando, Dine Agustin, Muhamad Irsan, Dina Fitria Murad, Hetty Rohayani, Dadang Sujana, Performance Comparison of Symmetries Encryption Algorithm AES and DES With Raspberry Pi, 978-1-7281-3880-0/19/$31.00 ©2019 IEEE*
4. *Bih-Hwang Lee, Ervin Kusuma Dewi, Muhammad Farid Wajdi, Data Security in Cloud Computing Using AES Under HEROKU Cloud, The 27th Wireless and Optical Communications Conference (WOCC2018)*
5. *Amjad Alsirhani, Peter Bodorik, Srinivas Sampalli, Improving Database Security in Cloud Computing by Fragmentation of Data,2017 International Conference on Computer and Applications (ICCA)*

6. *Tao Xiang a, Xiaoguo Li a, Fei Chen b, Yuanyuan Yang c, Shengyu Zhang achieving verifiable, dynamic, and efficient auditing for outsourced database in the cloud, J. Parallel Distrib. Computing,https://doi.org/10.1016/j.jpdc.2017.10.004 0743-7315/© 2017 Elsevier Inc. All rights reserved.*
7. *Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz, Performance Analysis of Different Cryptography Algorithms, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 3, March 2016 ISSN: 2277 128X.*
8. *Mr. Manish M Poteya,Dr C A Dhoteb,Mr Deepak H Sharmac,Homomorphic Encryption for Security of Cloud Data,7th International Conference on Communication, Computing and Virtualization 2016*
9. *S.Rajeswari,R.Kalaiselvi, Survey of Data and storage security in Cloud Computing, proceedings of 2017 IEEE International Conference on Circuits and Systems.*