# Review On Performance Evaluation Of Symmetric & Asymmetric Algorithm To Provide Security For Cloud Computing

Ashwini Gulhane
Assistant Professor,CSE DEPT.,
KGReddy College of Engineering,Moinabad,Hyderabad.
(DT), India.

***Abstract:*** As we are in time when the amenities of widespread connectivity, including the cloud, have put us at more risk than ever of getting hacked. When data goes into the wrong hands, the penalty can be shocking. High-profile data breaches and ransom ware attacks have organizations and individuals on red alert for the best ways to defend their data and networks, both now and for the future. While good IT security strategies can be very effective in protecting networks—essentially letting the good things in and keeping the bad things out—how do you account for all of the data that's traveling across the airwaves between mobile devices, browsers, databases, and the cloud? There's a time-tested science that is increasingly becoming a crucial link in the security chain: **encryption**. Encryption scrambles text to make it unreadable by anyone other than those with the keys to decode it, and it's becoming less of an added option and more of a must-have element in any security strategy for its ability to slow down and even deter hackers from stealing sensitive information. If good encryption is capable of hindering investigations by FBI experts, consider what it could do for you and your company's sensitive information. We can provide the good encryption only then when we will select an efficient algorithm; in this paper we review Symmetric and Asymmetric algorithms for security consideration on which one should be used for Cloud based applications and services that require data and link encryption.

***Keywords:*** **Cryptography, Security Algorithm, Symmetric, Asymmetric, RSA, RC6, AES, 3DES, MD5.**

## I. INTRODUCTION

Imagine two people who share critical secret information have to split up. This requires them to share and communicate their data and information from a distance, even as there lays a threat of an eavesdropper having the ability to stop, interfere or intercept their communications and seeks that same information. They decide to lock their information in a box using a lock that only the other knows the combination to and has the key to open it. The box is locked and sent over to the other user who uses the combination key to unlock the box and read its contents. In simple terms, Cryptography [1] can be seen as a method of storing and disguising confidential data in a cryptic form so that only those for whom it is intended can read it and are able to communicate information in the presence of an adversary and the security algorithms mitigate security issues by use of cryptography, authentication and distributing keys securely. Cryptography is the science of providing security for information. It has been used historically as a means of providing secure communication between individuals, government agencies, and military forces. Today, cryptography is a cornerstone of the modern security technologies used to protect information and resources on both open and closed networks. Thus the cryptography is the art of coding and decoding information between parties.
Cryptography involves the process of encryption and decryption. This process is depicted.

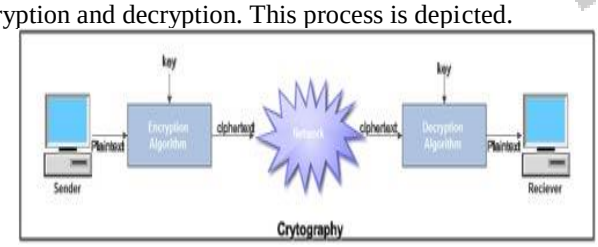


Figure 1: Cryptography Process

**Following security provided by the cryptography:**
**Confidentiality:** It is a set of rules that limits access to information also it relates to loss of privacy, unauthorized access to information and identity theft.
**Data Integrity**: It is the assurance that the information is trustworthy and accurate.
**Authentication:** It is the assurance that the parties involved in a real-time transaction are who they say they are.
**Non Repudiation:** It is the binding of an entity to a transaction in which it participates, so that the transaction cannot later be repudiated.
**Generally used terms in cryptography:**

**Plaintext** – Information that can be directly read by humans or a machine (this article is an example of plaintext).
**Cipher text** – The encrypted data.
**Encryption Algorithm:** It substitutes and performs permutations on plain text to cipher text.
**Decryption Algorithm:** It is encryption run in reverse by taking the secret key and transforming the cipher text to produce the original plain text.
**Keys**: It is used as input for encryption or decryption and determines the transformation.
**Sender and Recipients** are persons who are communicating and sharing the plaintext.

## II. SECURITY ISSUES

With respect to Cloud computing, the security concerns [2] are end user data security, network traffic, file systems, and host machine security which cryptography can resolve to some extent and thus helps organizations in their reluctant acceptance of Cloud Computing. There are various security threat are there ,the CSA (Cloud Security Alliance) listed the "Treacherous 12," the top 12 cloud computing threats organizations face in 2016. The CSA released the report to help both cloud customers and providers focus their defensive efforts. "The 2016 Top Threats release mirrors the shifting ramification of poor cloud computing decisions up through the managerial ranks," said J.R. Santos, executive vice president of research for the CSA.[3]

**Data breaches:**

Cloud environments face many of the same threats as traditional corporate networks, but due to the vast amount of data stored on cloud servers, providers become an attractive target. The severity of potential damage tends to depend on the sensitivity of the data exposed. Exposed personal financial information tends to get the headlines, but breaches involving health information, trade secrets, and intellectual property can be more devastating.

**Compromised credentials and broken authentication:**

Many developers make the mistake of embedding credentials and cryptographic keys in source code and leaving them in public-facing repositories such as GitHub. Keys need to be appropriately protected, and a well-secured public key infrastructure is necessary, the CSA said. They also need to be rotated periodically to make it harder for attackers to use keys they've obtained without authorization.

**Hacked interfaces and APIs:**

Weak interfaces and APIs expose organizations to security issues related to confidentiality, integrity, availability, and accountability because APIs and interfaces tend to be the most exposed part of a system because they're usually accessible from the open Internet.

**Exploited system vulnerabilities:**

System vulnerabilities, or exploitable bugs in programs, are not new, but they've become a bigger problem with the advent of multitenancy in cloud computing. Organizations share memory, databases, and other resources in close proximity to one another, creating new attack surfaces.

**Account hijacking:**

Phishing, fraud, and software exploits are still successful, and cloud services add a new dimension to the threat because attackers can eavesdrop on activities, manipulate transactions, and modify data. Attackers may also be able to use the cloud application to launch other attacks.[4]

## III. SECURITY ALGORITHM

To fight with above issues we have to select an efficient cryptographic algorithm following are the algorithm we have to use in cryptography.

a) **Private Key / Symmetric Algorithms: S**ingle secret key are used for encrypting large amount of data and are have fast processing speed. These algorithms use a single secret key that is known to the sender and receiver. RC6, 3DES, Blowfish, 3DES are some prime examples of this algorithms.
b) **PublicKey /Asymmetric Algorithms:** Use a key pair for cryptographic process, with public key for encryption and private for decryption. These algorithms have a high computational cost and thus slow speed if compared to the single key symmetric algorithms. RSA and Diffie Hellman are some types of public key algorithms.
c) **Signature Algorithms:** Used to sign and authenticate use data are single key based. Examples include: RSA, DH
d) **Hash Algorithms:** Compress data for signing to standard fixed size. Examples include: MD5, SHA.

## IV. ASYMMETRIC ALGORITHM

Asymmetric algorithm like (RSA, Elliptic curve, OAEP) which is used for security when data is transmitting over the network. These algorithms are based on digital signature scheme. [5]

### A. RSA (Rivest-Shamir-Adleman) :

The RSA algorithm is developed in 1977 by Rivets, Shamir, and Adelman (RSA). In this algorithm, one user (party) uses a public key and other user uses a secret key (private key) key. In the RSA algorithm each station independently and randomly chooses two large primes p and q number, and multiplies them to produce n=pq which is the modulus used in the arithmetic calculations of the algorithm[7]. The process of RSA algorithm is as follows [7].

1. Select p and q but both r prime numbers.
2. Calculate n= pq
3. Calculate z= (p-1)(q-1)
4. Select integer D which is relatively prime to 2. gcd ϕ (n)D= 1 (ϕ (n)= z)
5. Calculate ED= 1 mod (ϕ (n))
   For encryption: C = PE MOD N For Decryption: P = CD mod n , where C is the cipher text and P is the Plain text.

### B. DIFFIE–HELLMAN ALGORITHM

The Diffie–Hellman key exchange scheme was first published by Whitfield Diffie and Martin Hellman in 1976. Diffie– Hellman key exchange is a specific method of exchanging cryptographic keys. This method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel[8].Let us assume the A and B want to agree upon a key to be used for encryption / decrypting messages then The Diffie-Hellman key exchange algorithm works as follows:[9]

i. Firstly, A and B agree on two large prime numbers n and g. These two integers need not be kept secret. A and B can use an insecure channel to agree on them.
ii. A chooses another large random number x and calculates c such that C = gx mod n.

iii. A sends the number C to B .
iv. B independently chooses another large random integer y and calculate d such that D = gy mod n.
v. B sends number d to A.
vi. A now computes the secrete key K1 as follows: K1 = dx mod n.
vii. B now computes the secret key K2 as follows: K2 = cy mod n.

## V. SYMMETRIC ALGORITHM

Symmetric key algorithms are used primarily for the bulk encryption of data or data streams. These algorithms are designed to be very fast and have a large number of possible keys. The best symmetric key algorithms offer excellent secrecy; once data is encrypted with a given key, there is no fast way to decrypt the data without possessing the same key.
Symmetric key algorithms can be divided into two categories: block and stream. Block algorithms encrypt data a block (many bytes) at a time, while stream algorithms encrypt byte by byte (or even bit by bit).

**Problem faced with symmetric key algorithm:**

Firstly Symmetric cryptosystems have a problem of key transportation: The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging keys would be exchanging them personally.[10]

Another problem concerns the compromise of a private key [11] in symmetric- key cryptography; every participant has an identical private key. As the number of participants in a transaction increases, both the risk of compromise and the consequences of such a compromise increase dramatically. Each additional user adds another potential point of weakness that an attacker could take advantage of. If such an attacker succeeds in gaining control of just one of the private keys in this world, every user, whether there are hundreds of users or only a few, is completely compromised

Tools for cracking Symmetric encryption By use of Brute force [12] by running hacking tools that have the ability crack the combinations and keys to determine the plaintext message and perform Cryptanalysis where the attacks are focused on the characteristics of the algorithm to deduce a specific plaintext or the secret key. Then hackers are able to figure out the plaintext for messages that would use this compromised setup.

**Following are the symmetric Algorithm:**

**DES:**
DES is a block cipher. It encrypts data in blocks of size 64 bits each. 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. The key length is 64 bits [13].

**AES:**
AES is based on a design principle known as a substitution permutation network. AES has 128-bit block size and a key size of 128,192 or 256 bits [14] AES operates on a 4×4 column-major order matrixes of bytes, termed the state. Most AES calculations are done in a special finite field. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text. The number of cycles of repetition is as follows: a. 10 cycles of repetition for 128 bit keys. b. 12 cycles of repetition for 192 bit keys. c. 14 cycles of repetition for 256 bit keys. Each round of encryption process requires the following four types of operations: Sub Bytes, Shift Rows, Mix Columns, and XorRoundkey. Decryption is the reverse process of encryption and using inverse functions: InvSubBytes, InvShiftRows, and InvMixColumns [15].

**Blowfish**:
Blowfish is a 64-bit symmetric block cipher with variable length key. The algorithm operates with two parts: a key expansion part and a data-encryption part. The role of key expansion part is to converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes [16] The data encryption occurs via a 16-round Feistel network [17] It is only suitable for application where the key does not change often, like communications link or an automatic file encryption. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches.

## VI. RELATED WORK

With increasing security attack like malware, Ransomware, according to the survey done by the security company Kaspersky Lab recorded one ransomware attack every 40 seconds against companies in September and According to survey done by the the **PandaLabs report**, 18 million new malware samples were captured in this quarter alone, an average of 200,000 each day.
It has been noticed that because of this threats Cloud provider became more concern regarding security so they are giving more importance for security of end user data at the same time they are giving low priority for the cloud performance, due to this the performance of cloud is goes on decreasing because of inconsistent selection of algorithms for encryption and encoding.
By selecting the right cryptographic scheme end user data security can be achieved without losing out on cloud performance. Since Algorithm analysis is an essential in gathering the knowledge against any accidental or unintentional use algorithm that may prove to be inefficient or significantly impact application system performance due to encryption or decryption. For those cloud based web applications or portals needing real time or time sensitive data, an algorithm that might be taking a long time to long to run would prove a hindrance for the real time application as it may render the results to be useless. Such in efficient algorithm might end up needing lots of computing power or storage to execute over the cloud, making the algorithm useless in that environment.

In this paper [18] consider the performance of encryption algorithm for text files, it uses AES, DES and RSA algorithm and is evaluated from the following parameters.

- Computation time/Encryption time: The time is taken to convert plain text to cipher text is known as encryption time. According to [18] this paper RSA takes more time for computation process.

- Memory usage: It can be consider with the help of memory byte level. RSA takes larger memory than AES and DES.
- Output bytes: The output byte is calculated by the size of output byte of each algorithm. The level of output byte is equal for AES and DES, but RSA algorithm produces low level of output byte.

In another paper [19] Author compare AES, 3DES, Blowfish and DES. For comparison author used following parameter.

- Throughput:

Encryption time is calculated as the total plaintext in bytes encrypted divided by the encryption time. Decryption time is calculated as the total plaintext in bytes decrypted divided by the decryption time. As a result mentioned in the paper [19], it is said that Blowfish algorithm gives the better performance than all other algorithms in terms of throughput. The least efficient algorithm is 3DES.

In One more paper it has been discussed the performance evaluation of AES and BLOWFISH algorithms, and the parameters are Time consumption of packet size for 64 bit encodings and hexadecimal encodings, encryption performance of text files and images are compared with these two algorithms and calculate the throughput level,

Throughput of encryption = Tp/Et where Tp: total plain text (bytes),Et: encryption time (second)

The simulation results shows that Blowfish has better performance than AES in almost all the test cases.

## VII. EXPERIMENTAL RESULTS

The three audio files of different sizes are used to conduct experiments, where a comparison of three algorithms AES, RSA, BLOWFISH is performed. In this section, the AES, RSA and Blowfish algorithms can be implemented to different audio files. Comparison of encryption and decryption time for audio files has been given in the following table 1 and it shows the Throughput of AES, RSA and BLOWFISH algorithm for different audio files.

**Table1: Throughput of Audio files Encryption**

| Audio Files (MB) | AES (ms) | RSA (ms) | BLOW FISH(ms) |
|---|---|---|---|
| 4.01 | 150 | 200 | 180 |
| 3.02 | 140 | 180 | 170 |
| 6.28 | 240 | 400 | 256 |
| Average Time | 530 | 780 | 606 |
| Throughput(KB/ms) | 25.71 | 17.47 | 22.49 |

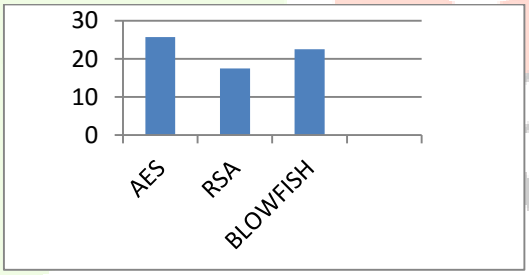


Fig. 2: Throughput of Audio files Encryption

Table 2: Throughput of Audio files Decryption

| Audio Files (MB) | AES (ms) | RSA (ms) | BLOW FISH (ms) |
|---|---|---|---|
| 4.01 | 200 | 300 | 230 |
| 3.02 | 180 | 230 | 200 |
| 6.28 | 310 | 500 | 340 |
| Average Time | 690 | 1030 | 770 |
| Throughput(KB/ms) | 19.75 | 13.23 | 17.70 |

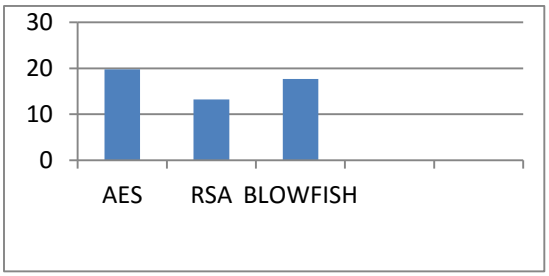


**Fig.3: Throughput of Audio files Decryption**

The simulation result for this comparison shown in Fig. 2 and Fig.3 .The result shown that AES algorithm is superior to other algorithm in terms of encryption time, throughput of the encryption and decryption process. Because more throughput more speed.

## VIII. CONCLUSION

This paper provides the review on symmetric and asymmetric algorithm also presents the performance evaluation of selected algorithm (AES, RSA, BLOWFISH).The presented simulation result show the frequent point's .Firstly it was concluded that AES algorithm has better performance than other algorithm followed by RSA and BLOFISH.

## REFERENCES

[1] Leena Khanna, Anant Jaiswal, "Cloud Computing: Security Issues and Description of Encryption Based Algorithms to Overcome Them", IJARCSSE 2013.
[2] Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Naslund, Makan Pourzandi "A quantitative analysis of current security concerns and solutions for cloud computing", Springer 2012.
[3] Cloud Security Alliance (CSA), "Security Guidance for critical Areas of Focus in cloud computing V3.0" CSA 2016.
[4] https://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html
[5] Neha Garg, Partibha Yadav, " Comparison of Asymmetric Algorithms in Cryptography" , International Journal of Computer Science and Mobile Computing, April- 2014.
[6]William Stalling, "Cryptography and Network Security Principal and Practice", Third Edition, Pearson 2006.
[7] Prashant Kumar Arya, Dr Mahendra Singh Aswal and Dr Vinod Kumar," Comparative Study of Asymmetric Key Cryptographic Algorithms" , International Journal of Computer Science & Communication Networks",Vol 5(1),17- 21, ISSN:2249-5789.1.
[8] W. Stallings, "Cryptography and Network Security Principles and Practices", Fourth Edition, Pearson Education, Prentice Hall, 2010.
[9] Nitin Jirwan, Ajay Singh and Dr. Sandip Vijay,(March - 2013)," Review and Analysis of Cryptography Techniques", International Journal of Scientific & Engineering Research Volume 4, Issue3.
[10] William Stalling, "Cryptography and Network Security Principal and Practice", Third Edition, Pearson 2006.
[11] W. Küchlin, "Public key encryption," ACM SIGSAM Bulletin, August 1987, pp. 69- 73
[12]Akashdeep Bhardwaja, GVB Subrahmanyamb , Vinay Avasthic , Hanumat Sastryd," Security Algorithms for Cloud Computing" International Conference on Computational Modeling and Security (CMS 2016)
[13] "DESalgorithm" http://orlingrabbe.com/des.htm
[14] Atul Kahate, "cryptography and network security", Tata McGraw-Hill publishing company, New Delhi, 2008.
[15] William Stallings, "cryptography and network security", pearson prentice hall, 2006, 4th edition..
[16] "Blowfish Algorithm" Available:
http://www.schneier.com/blowfish. html.
[17] "BLOWFISHalgorithm" http://pocketbrief.net/related/BlowfishEncryption.pdf
[18] Shashi Mehrotra Seth, Rajan Mishra, "Comparitive Analysis of Encryption Algorithms For Data Communication", IJCST Vol.2, Issue 2, June 2011.
[19] "Performance Analysis of AES and BLOWFISH Algorithms", National Conference on Computer Communication & Informatics", School of computer science, RVS college of arts and science, March 07, 2012.