International Journal on Emerging Technologies (Special Issue NCETST-2017) **8**(1): 746-750(2017)
(Published by Research Trend, Website: www.researchtrend.net*)*

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Comparative Study of Different Cryptographic Algorithms for Data Security in Cloud Computing

***Mr. Pradeep Semwal*[1] *and Dr. MK Sharma*[2]**
[1]*Research Scholar (CSE) Uttarakhand Technical University, Dehradun, (UK), INDIA*
[2]*Associate Prof, Dept. of Comp Application Amrapali Institute, Haldwani, Nainital, (UK), INDIA*

ABSTRACT: In the word of internet in every second huge amount of data being generated everyday on the internet and stored in the cloud. Securing information stored in the cloud is a biggest challenge. Cryptography is very useful to ensure privacy & information security for making internet a safer place. Cryptography is a process of making information unintelligible to an unauthorized person. Hence, providing confidentiality to the authorized users. There are various cryptographic algorithms that can be used. Ideally, a user needs a cryptographic algorithm which is of low cost and high performance. However, in reality there is no such algorithm which is a one stop solution of all. Thus, amongst the various cryptographic algorithms existing, we choose an algorithm which best fits the user requirements. In, this process of choosing a study of strengths, weakness, cost and performance of each algorithm will provide valuable insights. In this paper, we have implemented and analyzed in detail cost and performance of popularly used cryptographic algorithms like DES, 3DES, AES, RSA and blowfish to show an overall performance analysis.

Keywords: Cryptography, Symmetric Algorithms, Asymmetric Algorithms, AES, DES, RSA and BLOWFISH, Encryption Decryption time, Avalance effect, Entropy.

I. INTRODUCTION

Cryptography also termed as an art of concealing information so that only the authenticated parties can have access to the private information.

In the Cryptography basic elements are Plain text and Cipher text. Plain text in the original data which the sender wants to send and Cipher text is the encrypted format of the plain text. The plain text is converted to the Cipher text using encryption algorithms and cipher text is converted back to plain text using decryption algorithm. These algorithms are mainly classified into two types symmetric key algorithm and asymmetric key algorithm. In this paper, different encryption algorithms are discussed along with their applications.

The paper first discusses different symmetric key & asymmetric key algorithms then a comparative analysis of the above algorithms is various parameters.

II. SYMMETRIC KEY ALGORITHMS

Symmetric algorithm is also called secret key algorithm. The sender and the receiver share the same key for encryption and decryption. This shared secret key needs to be kept secured by both the parties otherwise any one can steal the data in between the transmission .

There are different types of symmetric key algorithms like Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES) and Blowfish.

A. Data Encryption Standard (DES) Algorithm

Data Encryption Standard (DES) is a symmetric key algorithm which was developed by IBM in 1977. It uses key of size 56-bits to encrypt the plain text block of size 64 bit. It consists of a *fiestal* network which divides a block into two equal halves where the right half passes through a various function. DES uses a chain of S-boxes and P-boxes. After passing through these permutation and substitution box the cipher text is obtained by the XOR operation .DES uses 19 rounds.

Decryption is just the reverse process of encryption. DES is not a good algorithm to trust on as it is vulnerable to brute force attacks. The DES algorithm has been modified (called M-DES) to improve the Bit Error Rate(BER) caused due to avalanche effect and is made more secure so that it can be used in wireless communication. For modification the authors have made use of S-box mapping tables. The second modification has been done from the work in where the authors have shown that DES can be cracked from the differential cryptanalysis attack. The BER [Bit Error Rate] in M-DES is much better than DES, because there is no Avalanche effect in M-DES so came out with good results but it is vulnerable to Men in Middle attack.

B. Triple Data Encryption Standard (3DES) Algorithm

Triple Data Encryption Standard also called as 3DES was introduced by IBM in 1978 to enhance the security of the data. It uses block size of 64-bits with a key length of 56bits. As the name suggests it performs the same DES algorithm but three times to each data block. Although the algorithm is vulnerable to brute force attack but it is comparatively more secure than DES and 2DES.It was mainly designed to make it secure form Men in Middle attack.

Now a day's 3-DES is used in many applications, so some measures must be taken to implement it in a modified form.

C. Advanced Encryption Standard (AES) Algorithm

There are certain vulnerabilities in DES and 3DES, so NIST (National Institute of Standard and Technology) developed a new algorithm called Advanced Encryption Standard (AES).

AES work on blocks of three different sizes 128 bit, 192 bit and 256 bits .AES -128 uses 10 rounds, AES-192 has 12 rounds and AES-256 consist of 14 rounds. Each round goes through a series of steps like substitution byte, shift rows, mixed columns and add round Key. AES Algorithm is comparatively more secure and has a strong avalanche effect. Attackers cannot easily decrypt the encrypted text by the brute force attack. Therefore AES has been used in many applications like it is used PDA communication .There are many attacks on AES algorithm ,one such attack which is a combination of boomerang and rectangle attack with related key differentials . This attack can break the round versions of AES but not complete AES. There are attacks which occur due to the vulnerability of S-box in AES algorithm.

A modified version of AES was introduced to carry out MPEG video encryption [18]. The algorithm was modified to overcome calculations and computation overhead.

D. Blowfish Encryption Algorithm

Blowfish Algorithm , one of the most efficient algorithm was developed by Bruce Schneier in 1993 It has a variable key length maximum up to 448 bits. It has a block size of 64-bits. Blowfish algorithm consists of two phases. The first phase is key expansion phase, in this phase 448 bit key is converted into number of sub keys totaling 4168 bytes [19].The second phase is encryption phase, a function is iterated 16 times and the encrypted text is obtained using XOR operation. Blowfish is a strong encryption algorithm so it has been used in many applications.

Certain tests [20] were applied to check the performance of blowfish algorithm by increasing the file size and the key length . The Password Management System is also based on Blowfish Algorithm [21].The algorithm has also been used in bitmap image plotting in place of secret algorithms like Skipjack algorithm in the Clipper and Capstone chips [22], [23]. Performance was also evaluated by modifying its function which brought up good results discussed in [26].

III. ASYMMETRIC KEY ALGORITHM

We have discussed very powerful & widely used asymmetric algorithms in this section.

Asymmetric Key Algorithm is also called public key cryptography. It uses two keys 'Private Key' and 'Public key'. The sender before transmission encrypts the plain text with the help of public key to produce cipher text and the receiver decrypts this cipher text with the help of its private key. One such powerful asymmetric algorithm is Rivest Shamir Adlemen (RSA).

A. Rivest Shamir Adlemen (RSA)

The algorithm was developed by Rivest, Shamir and Adlemen in 1977. It is a public key algorithm because it uses two keys one to encrypt and other to decrypt the message. Public key is used by the sender to the private key (only known to receiver) is used by the receiver to decrypt the message. This private key, as the name suggests is known only to the receiver. The RSA consists of some mathematical operations through which it can calculate the encryption and decryption keys (E and D), after that one can easily calculate the cipher text and the plain text by the following formula.

$C = M^{E} \bmod(n)$……. (1)

$P = M^{D} \mathrm{mod}(n)$…… (2)

Where E & D are public and private keys and n is a value obtained from mathematical operations in RSA . To carry out performance analysis RSA was modified. Although RSA is a secure algorithm,

but in [29] an experiment was done in the application of low private exponent attack in RSA where the author found out that there can be some new weak keys in RSA. Therefore, digital signature concept was introduced in combination with RSA [30]. So algorithm implementing Digital Signature with RSA Algorithm [31] was proposed to double the security of the algorithm. The RSA has been used in various applications like in e-com which ensure message integrity, privacy, authentication and non-repudiation. In the next section, a comparative analysis of different algorithms is given.

IV. COMPARATIVE ANALYSIS

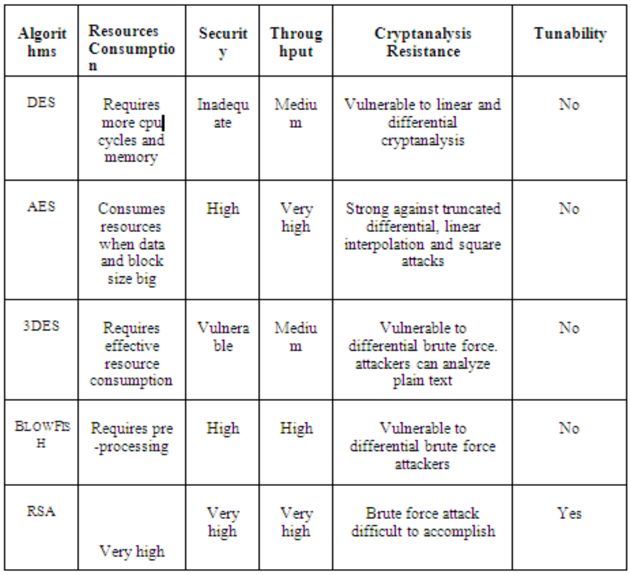
The Table 1 & Table 2 shows the comparative analysis between different symmetric and asymmetric algorithms at different attributes such as the key length, block size, rounds, power consumption, avalanche effect, processing time & resource consumption.

In [34] the authors have encrypted files with different contents and sizes. The results proved that Blowfish showed a good performance than the other encryption algorithms and therefore the processing time of the blowfish algorithm was high. AES performance was better than DES and 3DES and it took less time in encryption and decryption. Next property, Avalanche effect is a property of block ciphers in which the output bits change significantly on a slight change of the input bits. Blow fish has a maximum avalanche effect due to the number of XOR operations which changes the output drastically. DES has avalanche lower than AES [35]. RSA also has high avalanche effect as it involves the mathematical calculation of two large prime numbers. Now, talking about cryptanalysis resistance, authors have explained differential cryptanalysis for each of the algorithm. It was observed that DES is highly vulnerable to linear and differential cryptanalysis. It was also found that 3DES and Blowfish were vulnerable to brute force attacks whereas in case of RSA brute force attack was difficult. AES proved to be strong against differential, linear interpolation and square attacks [36]. Therefore the crack to AES algorithm has not been found yet. Comparing with the other algorithms only DES is the most insecure algorithm as it has already been declared inadequate to use.

Table1 & Table 2

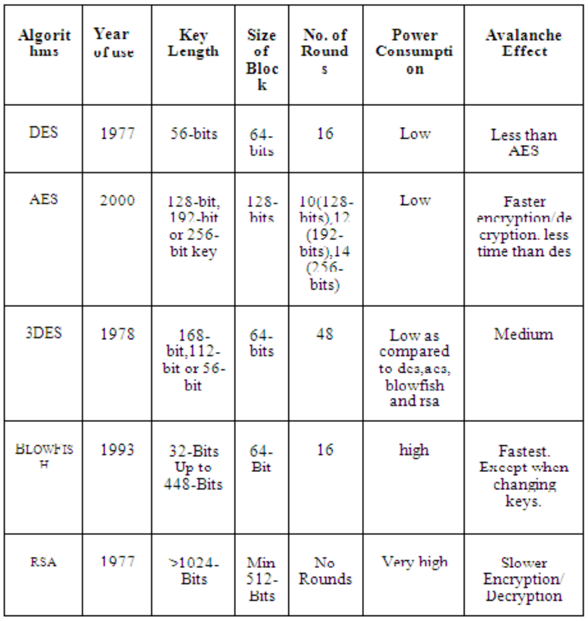
: Comparative analysis of different cryptography algorithms

Table 1



Algorithms	Resources Consumption	Security	Throughput	Cryptanalysis Resistance	Tunability
DES	Requires more cpu cycles and memory	Inadequate	Medium	Vulnerable to linear and differential cryptanalysis	No
AES	Consumes resources when data and block size big	High	Very high	Strong against truncated differential, linear interpolation and square attacks	No
3DES	Requires effective resource consumption	Vulnerable	Medium	Vulnerable to differential brute force. attackers can analyze plain text	No
BLOWFISH	Requires pre -processing	High	High	Vulnerable to differential brute force attackers	No
RSA	Very high	Very high	Very high	Brute force attack difficult to accomplish	Yes

Table 2



Algorithms	Year of use	Key Length	Size of Block	No. of Rounds	Power Consumption	Avalanche Effect
DES	1977	56-bits	64-bits	16	Low	Less than AES
AES	2000	128-bit, 192-bit or 256-bit key	128-bits	10(128-bits),12 (192-bits),14 (256-bits)	Low	Faster encryption/decryption. less time than des
3DES	1978	168-bit,112-bit or 56-bit	64-bits	48	Low as compared to des,aes, blowfish and rsa	Medium
BLOWFISH	1993	32-Bits Up to 448-Bits	64-Bit	16	high	Fastest. Except when changing keys.
RSA	1977	>1024-Bits	Min 512-Bits	No Rounds	Very high	Slower Encryption/ Decryption

V. IMPLEMENTATION

We have implemented and compared DES, 3DES, AES, blowfish and RSA algorithms in java using Eclipse IDE.

We have used java inbuilt packages like java security and java crypto which provides security features like encryption, decryption, key generation, message authentication and authorization. We have used files with text and images of sizes 25KB, 50KB, 1 MB,2MB,3MB.For sake of comparison we have used the same input files for all algorithms throughout the experiment. We have used assame system for all implementations and analysis work, so that memory and processor conditions. All block cipher algorithms are set in mode ECB. The method of implementing algorithms using functions of java.security and java.crypto package is as follows:-

Generatekey() using keygenerator class, createacipher object() with parameters algorithm name and mode, initializethecipher() created for encryption / decryption and perform encryption/ decryption using doFinal()method.

VI. EVALUATION PARAMETERS

Each of the encryption techniques has its own strong and weak points. In order to apply a suitable cryptography algorithm to an application, we should have knowledge regarding performance, strength and weakness of the algorithms. Therefore, these algorithms must be analyzed based on several features. In this paper, analysis is done with following metrics under which the cryptosystems can be compared: Encryption time, Decryption time, Avalanche effect, Memory used

VII. RESULTS AND DISCUSSIONS

In this section we discuss the results obtained from implementation in java based on above four evaluation parameters.

A. Encryption time

Experiment and the fig 1 reveal that RSA takes highest time for encryption, and blowfish takes least time for encryption,

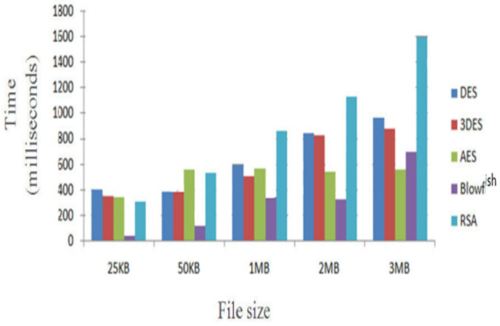


Fig.1. Encryption time vs. File size for DES, 3DES, AES, Blowfish and RSA.

B. Decryption time

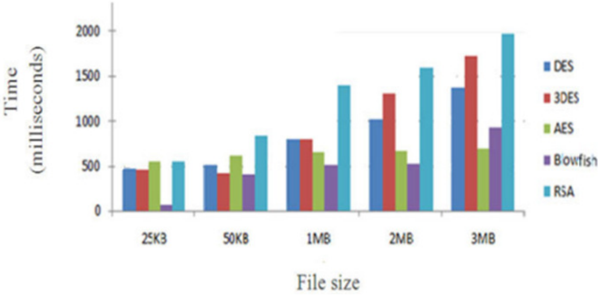


Fig. 2. Decryption timevs. Filesize for DES, 3DES, AES, Blowfish and RSA.

Fig. 2. shows that among all algorithms, RSA takes highest time and blowfish takes least time for decryption

C. Memory Consumption

Table 3.

Algorithm	Memory consumed(KB)
DES	18.2
3DES	20.7
AES	14.7
Blowfish	9.38
RSA	30.5

Table 3 shows that memory used for unit operations for listed algorithms.

D. Avalanche Effect

In cryptography, a property called diffusion reflects cryptographic strength of an algorithm. If there is a small change in an input the output changes significantly. This is also called avalanche effect. We have measured Avalanche effect using hamming distance. Hamming distance is measure of dissimilarity. We find hamming distance as sum of bit by XOR considering ASCII value. A high degree of diffusion i.e. high avalanche effect is desired. Avalanche effect reflects performance of cryptographic algorithm.

Avalanche effect = (hamming distance ÷file size)

Avalanche effect tells us the degree of diffusion of information. A change of one bit in plain text leading to significant change in bits of output information. AES uses a substitution permutation network using multiplicative inverse and affine transformation.

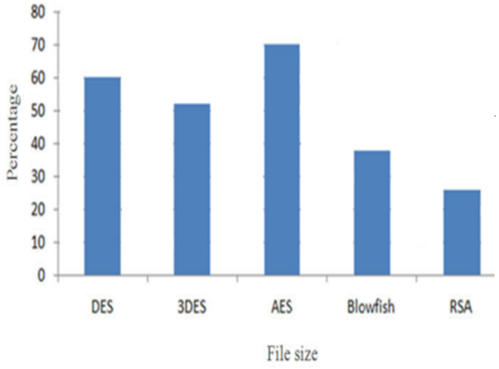


Fig. 3. Shows that AES has highest Avalanche effect where as RSA shows least Avalanche effect.

VIII. CONCLUSION

Each encryption algorithm has its own strong and weak points. From the experiment results shows

-Blowfish is best in terms of memory requirement whereas RSA has a large memory requirement, so blowfish can fit well in small application specially in embedded applications.

-As for encryption time is concerned RSA consumes maximum time as compare to other cryptographic algorithm whereas blowfish has least encryption time.

-The avalanche effect of AES is maximum, so AES can be preferred for application where privacy and integrity of the message is of top priority.

-The bandwidth consumption of AES is highest for the transmission of encrypted message where as it is least for DES.

REFERENCES

[1]. T. Bala and Y. Kumar, "Asymmetric Algorithms and Symmetric Algorithms: A Review," *International Journal of Computer Applications* (ICAET), pp.1-4, 2015.

[2]. W. Stallings, Cryptography and Network Security, 4th Ed, pp. 58-309, Prentice Hall,2005.

[3]. W. Y. Zibideh and M. M. Matalgah, "Modified-DES Encryption Algorithm with Improved BER Performance in Wireless Communication," *IEEE Radio and Wireless Symposium (RWS)* Phoenix, pp. 219-222 , Jan 2011.

[4]. H. Yoshikawa, M. Kaminaga, A. Shikoda, and T. Suzuki, "Round addition DFA for microcontroller implemented the Triple DES," IEEE Consumer Electronics (GCCE) Tokyo, pp. 538-539, October2013.

[5]. W.Y Zibideh. and M. M. Matalgah, "An Optimized Encryption Framework based on the Modified-DES Algorithm: A Trade-Off between Security and Throughput in Wireless Channels," *IEEE Radio and Wireless Symposium (RWS)* CA, pp.419-422, January, 2012.

[6]. E. Biham and A. Shamir, "Differential Cryptanalysis of the Full 16- Round DES," Proceedings of Crypto' **92**, vol. 740, Santa Barbara, CA, December1991.

[7]. P. Kitsos, S. Goudevenos and O. Koufopavlou, "VLSI implementations of the triple-DES block cipher," *IEEE Electronics Circuits and Systems*, Vol. **1**, pp.76-79, December 2003.

[8]. NIST Special Pubilication 800-20, "Modes ofOperation Validation System for the Triple Data Encryption Algorithm," National Institute of Standard and Technology, 2000.

[9]. LIU Niansheng , G. Donghui, and H. Jiaxiang, "AES Algorithm Implemented for PDA Secure Communication with Java," *IEEE Anti-counter. Sec. Ident. Fujian*, pp. 217-222, April 2007.

[10]. E. Biham, O. Dunkelman, and N. Keller, "Related-Key Boomerang and Rectangle Attacks," Lecture Notes in Computer Science, vol. **3494**, pp. 507-525,Berlin: Springer-Verlag, 2005.

[11]. Y. A. Zhang and D.G. Feng, "Equivalent Generation of the S-box of Rijndael," *Chinese J. Computers,* Vol. **27**, no.12, pp.1593-1600, December 2004.

[12]. W. Millan, "How to Improve the Nonlinearity of Bijective S-boxes," Lecture Notes in Computer Science, Vol. **1438**, pp.181 - 192, Berlin: Springer-Verlag, 1998.

[13]. Chen and D. G. Feng, "An Evolutionary Algorithm to Improve the Nonlinearity of Self-inverse S-Boxes," Lecture Notes in Computer Science, vol. **3506**, pp.352- 361, Berlin: Springer-Verlag, 2005.

[14]. J. M. Liu, B. D. Wei, and X.G. Cheng, "An AES SBox to Increase Complexity and Cryptographic Analysis, " *IEEE Proc. of the 19th International Conference on Advanced Information Networking.*