Analytical Comparison of Symmetric Encryption and Encoding Techniques for Cloud Environment

Krunal Suthar
Patel Institute of Technology
Ratibad, Bhopal.

Parmalik Kumar
Patel Institute of technology,
Ratibad, Bhopal

Hitesh Gupta
Patel Institute of Technology
Ratibad, Bhopal

Hiren Patel
S. P. College of Engg.
Visnagar, Gujarat

ABSTRACT

Cryptography in the field of information technology is an art to protect data privacy using standard mathematical techniques. Cloud computing, one of the emerging techniques to lease computing resources on demand, makes use of remote data storage where data owner does not possess direct control over her data. To protect privacy of users' data and to enable user to verify integrity of the data stored on remote location, modern cryptographic techniques are used. Cryptographic techniques impose computational and communication overhead which in turn affect the performance of the overall operation. In this research article, we analyze two broad categories of cryptography viz. symmetric key encryption and encoding. We analyze various algorithms and compare them on the basis of security and performance perspectives. We further make recommendations for Cloud users to protect & verify their sensitive data using one of these cryptographic techniques..

General Terms

Security.

Keywords

Cloud Computing, Data Security, Privacy, Encryption, Encoding, Performance.

1. INTRODUCTION

Storage as a service is one of the significant services offered by Cloud computing where the user stores her data online on cloud without keeping the local copy of the same at her premise. While doing so user loses her direct control over the data. Data stored on the cloud may be tempered by an unauthorized entity or sometimes by the Cloud service provider itself, accidently or intentionally. To protect confidentiality of data one may encrypt the same, using one of the modern encryption techniques available, before sending it to cloud server. There are a wide range of encryption algorithms (e.g. AES, DES, TDES, Blowfish) available which are secure enough and used to make data secure by converting it to unreadable format. For verifying the integrity of the data encoding techniques such as hash code or MAC (E.g. MD5, or SHA-1) can be used. Thus, the combination of encryption and encoding is widely being used to achieve confidentiality schemes available (e.g. AES, DES, or TDES) as well Encoding schemes (e.g. SHA256, MD5) based on sensitivity of her data.

and integrity. Incorporating such cryptographic techniques results into computational and communication overhead which in turn affects the overall performance of the cloud system. It is of utmost importance to understand these computational overhead for various algorithms and recommend appropriate schemes under different situation.

In this paper our aim is to study and analyze some widely used symmetric encryption and encoding techniques and to compare them based on some factors viz. performance and security. The rest of the paper is organized as follows. Section 2 contains details of related work followed by Section 3 defining problem statement. Section 4 provides experimental design. Section 5 shows results and other important comparisons. Section 6 contains conclusion & future work and followed by list of references used.

2. RELATED WORK

Data security in cloud computing is rising trust area in research work. It was concluded in [2] that AES is faster and more efficient cryptographic algorithms. When the data transmission is considered there is insignificant difference in performance of different symmetric key schemes. A study in [3] conducted for different popular secret key algorithms as DES, AES, and Blowfish. They were implemented, and their performance was compared by encryption input files of varying contents and sizes.

A researcher at [10] gives comparative study between DES, AES and Triple DES based on nine factors, Which are key length, cipher type, block size, developed, cryptanalysis resistance, security, possibility key, possible ACSII printable character keys, time required to check all possible key at 50 billion second etc, and based on all concluded that the AES is better than DES and Triple DES.

3. PROBLEM STATEMENT

Researchers of Cloud storage security are giving more focus on how to make data more secure and giving less attention towards degradation of Cloud performance due to not selecting proper encryption and Encoding algorithms. So, if users paying awareness in selection of proper cryptographic scheme then it can achieve confidentiality without losing performance of Cloud. For Achieving high performance and security users can select any of modern symmetric encryption

4. EXPERIMENTAL DESIGN

In our experiment comparison of three Symmetric encryption algorithms that's AES, DES and Triple DES as well encoding algorithm like SHA256, MD5 to be made. Performance of algorithms is evaluated based on the following parameters.

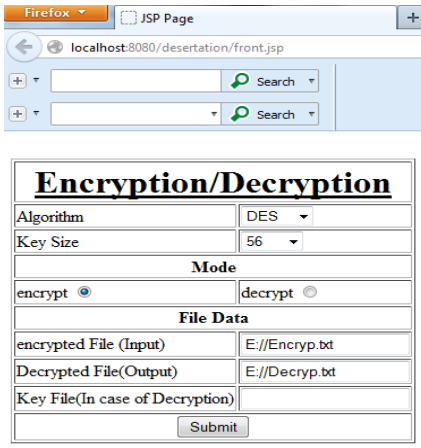
A. File Size

B. Computation (Encryption) Time

C. Computation (Encoding) Time

The File size indicate file of different size to be taken, computation time is considered the time that an encryption algorithm takes to produces a cipher text from a plain text (i.e. File) and encoding time is time taken by encoding algorithm to produce a hash code. System are coded using Java programming language, compiled with Net beans IDE, and run on a Core 2 Duo 1.73 GHz processor under Windows 7 environment.

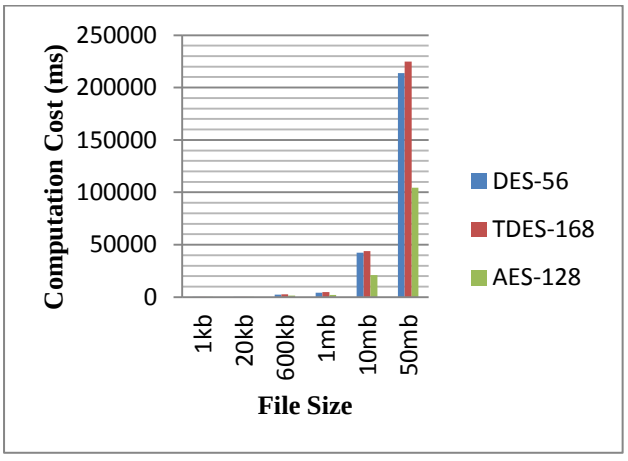
Figure 1 : Simulation Screenshot



5. RESULTS

Experimental results of comparison for selected Symmetric Encryption algorithm are shown below by giving different file size as an input and record computation cost.

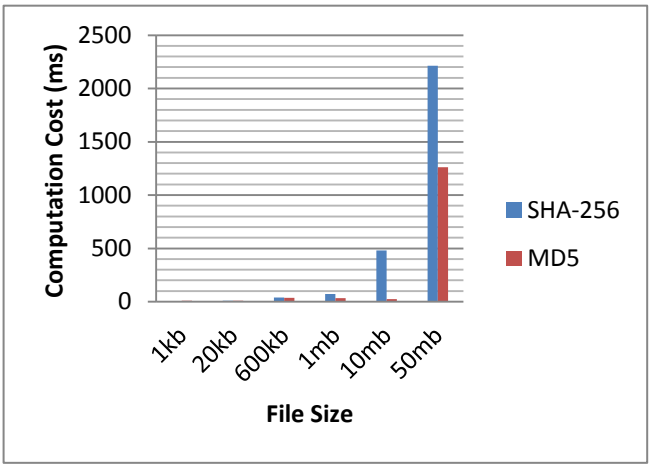
Figure 2: File size v/s Computation Cost



From figure2 we can say that and AES is work faster than other two schemes.

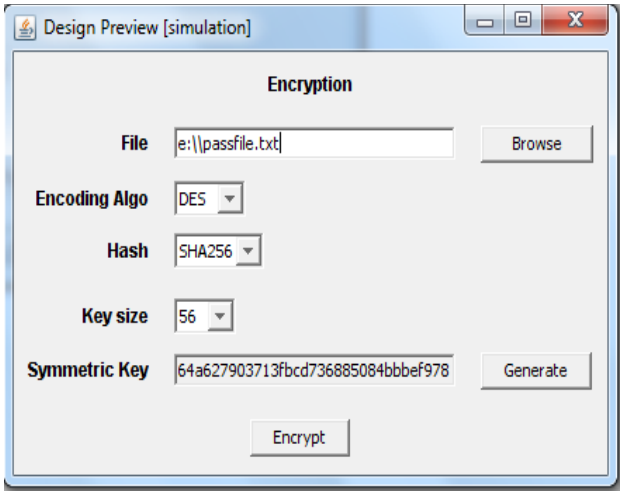
Now let we focus on Encoding scheme which produce a fixed size message digest(Hash). Figure 3 below shows computation cost for two widely used data Encoding scheme.

Figure 3: SHA- 256 V/S MD5



From Figure3 we can say that MD5 work faster than SHA256. In this paragraph let we discuss about round trip time that is calculated by implementing a Cloud simulation using JAVA RMI technique.

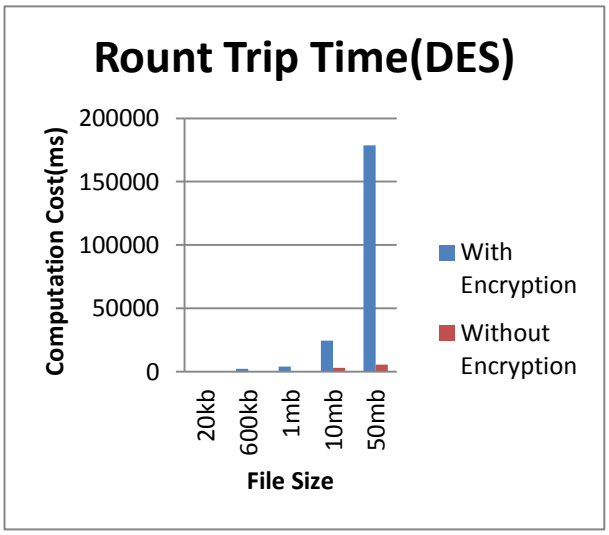
Figure 4 : Cloud Simulation



We use different algorithm to encrypt the file and check the total time that is summation of time required to reading file, Encrypting it, create chunk, Sending, Storing it on Cloud and receiving confirmation. The figure4 above shows Cloud Simulation.

Below figure5 shows a graph for encrypting different file using DES algorithm that is calculated using Cloud suit. This statistics shows that the major time is required by the encryption mechanism. So, if we use the encryption technique which works fast we can improve the efficiency of Cloud environment.

Figure 5 : Comparison With Encryption/ Without Encryption



Now, take the look on security part of all this techniques. As, In Cloud environment user needed as much as possible security for their data. The security provided by algorithm is more depends on the length of key being used. DES encrypts data in 64 bit block size and uses effectively a 56 bit key. 56 bit key space amounts to approximately 72 quadrillion possibilities. Even though it seems large it is not sufficient and vulnerable to brute force attack. Somewhat solution is given by Triple DES which is secure enough compare to DES. Triple DES is an assembly of applying DES three times so more secure towards brute force type of attack and work with 112/168 bit of key. Even DES/Triple DES provide enough security AES provide some more benefits. AES works fast even on small devices such as smart phones; smart cards etc. as well provides enough security due longer key size.

Encoding algorithm is used to check the integrity or say correctness of data while data is available on Cloud server. A SHA256 are more secure than MD5 coz SHA256 produce a 160 bit (20byte) message digest while MD5 produce a 128 bit (16 byte) message digest. Larger digest size produce by SHA256 makes it stronger against various types of attacks.

Table1 shows the security Comparison among various symmetric encryption techniques. Based on factors like Key size, Speed, Attacks, Number of Rounds Etc.

Table 1: Security comparison[9][15]

Algorithm	Key size(s)	Speed	Speed depends on key size?	Attacks	Round	Comment
AES	128, 192, 256	Fast	Yes	Side Channel Attacks	9,11, 13	It's good to allowing a 256-bit key size, which should protect against certain current and future attacks.
DES	56	Slow	–	Brute Force Attack	16	more vulnerable for Brute force attack compare to AES/Triple DES due to small key size(i.e 2^{56} comparison)
Triple DES	112/ 168	Very slow	No	Theoretically possible	48	More secure compare to DES and less vulnerable coz algorithm applying three times with different key to secure data.

6. CONCLUSION AND FUTURE WORK

Modern cryptographic techniques such as encryption and encoding are widely used in Cloud computing to protect confidentiality and integrity of the users' data stored on cloud. These algorithms result into computational overhead which affect the performance of the cloud. We have analyzed AES, DES & 3DES symmetric encryption techniques and MD5 & SHA-256 encoding techniques. AES is one of the good candidates for symmetric key encryption, where as DES and 3DES produces more overhead. In case of encoding, MD5 is faster but SHA seems to be more secure. Instead of providing flat options for encryption and encoding, we recommend taking an option from cloud data owner about sensitivity of her data and performance required for the same.

This user input can be used to select combinations of these cryptographic primitives. In future we wish to include asymmetric key encryption technique in our pool of algorithms. We also wish to include more file formats especially used on social networking in our datasets.

REFERENCES

[1] Shashi Mehrotra Seth, Rajan Mishra "Comparative Analysis Of Encryption Algorithms For Data Communication" In *IJCST Vol. 2*, Issue 2, June 2011.

[2] S. Hirani, "Energy Consumption of Encryption schemes in wireless device" *Thesis, university of Pittsburgh*, Retrieved Oct.1, 2008.

[3] A.Nadeem, "A performance comparison of data encryption algorithms", *IEEE information and communication technologies*, 2006.

[4] Anoop MS, "Public key Cryptography (Applications Algorithm and Mathematical Explanations)"

[5] Diaasalama AbdElminaam, Hatem Mohamad Abdual Kader, Mohly Mohamed Hadhoud, "Evalution the Performance of Symmetric Encryption Algorithms", In *IJNS May 2010*.

[6] Erik Olson, Woojin Yu, "Encryption for Mobile Computing".

[7] Neetu Settia. "Cryptanalysis of modern Cryptography Algorithms". In *IJCS*T. 2010.

[8] http://www.javamex.com/tutorials/cryptograp- hy/ciphers. shtml.

[9] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani "New Comparative Study Between DES, Triple DES and AES within Nine Factors" In *JOURNAL OF COMPUTING*, 2010.

[10] Ayushi "A Symmetric Key Cryptographic Algorithm" In *International Journal of Computer Applications* 2012.

[11] Priya Dhawan., "Performance Comparison: Security Design Choices," *Microsoft Developer Network* October 2002.

[12] basics of cryptography, fisher.osu.edu /~muhanna_1/pdf/crypto.pdf.

[13] Schneier, B. (1996), "*Applied Cryptography"*, Wiley & Sons, p. 399.

[14] M. Blaze, W. Diffie, R.L. Rivest, B. Schneier, T. Shimomura, E. Thompson, M. Wiener, "Minimal key lengths for symmetric ciphers to provide adequate commercial security" January 1996.

[15] Monika Agrawal "A Comparative Survey on Symmetric Key Encryption Techniques "In *International Journal on Computer Science and Engineering (IJCSE)* Vol. 4 No. 05 May 201 2.